Explicit open image theorems for abelian varieties with trivial endomorphism ring

Davide Lombardo*
Département de Mathématiques d'Orsay

Abstract

Let K be a number field and A/K be an abelian variety of dimension g with $\operatorname{End}_{\overline{K}}(A) = \mathbb{Z}$. We provide a semi-effective bound $\ell_0(A/K)$ such that the natural Galois representation attached to $T_\ell A$ is onto $\operatorname{GSp}_{2g}(\mathbb{Z}_\ell)$ for all primes $\ell > \ell_0(A/K)$. For general g the bound is given as a function of the Faltings height of A and of the residual characteristic of a place of K with certain properties; when $g = 3$, the bound is completely explicit in terms of simple arithmetical invariants of A and K.

1 Introduction

Let K be a number field and A be a K-abelian variety. The purpose of the present work is to study the Galois representations attached to A under the assumption that $\operatorname{End}_{\overline{K}}(A)$ is $\mathbb{Z}$. More precisely, we are interested in the family of representations

$$\rho_{\ell^\infty} : \operatorname{Gal}\left(\overline{K}/K\right) \to \operatorname{Aut}(T_\ell(A)) \cong \operatorname{GL}_{2g}(\mathbb{Z}_\ell)$$

arising (after a choice of basis) from the ℓ-adic Tate modules of A. We shall also consider the residual mod-ℓ representations $\rho_\ell : \operatorname{Gal}\left(\overline{K}/K\right) \to \operatorname{Aut}(A[\ell]) \cong \operatorname{GL}_{2g}(\mathbb{F}_\ell)$, and write G_{ℓ^∞} (resp. G_ℓ) for the image of ρ_{ℓ^∞} (resp. of ρ_ℓ). By work of Serre [Ser86] and Pink [Pin98] many results are known on these representations: in particular, we know that if – for some prime ℓ – the Zariski closure of G_{ℓ^∞} has rank $g+1$, then the same is true for all primes, and in fact the equality $G_{\ell^\infty} = \operatorname{GSp}_{2g}(\mathbb{Z}_\ell)$ holds for all ℓ large enough (with respect to A/K). Furthermore, if we assume the Mumford-Tate conjecture, this condition is equivalent to the Mumford-Tate group of A being $\operatorname{GSp}_{2g,\mathbb{Q}}$, and even better, if $g = \dim A$ lies outside a certain very thin set, then the condition $\operatorname{MT}(A) = \operatorname{GSp}_{2g,\mathbb{Q}}$ is automatically satisfied and the Mumford-Tate conjecture is true for A (cf. theorem 1.4 below).

Our aim is to make these results explicit, by finding a bound $\ell_0(A/K)$ (which, as the notation suggests, will depend on A and K) such that, for all primes $\ell > \ell_0(A/K)$, the representation ρ_{ℓ^∞} is onto $\operatorname{GSp}_{2g}(\mathbb{Z}_\ell)$. To state our results more compactly we introduce the following functions:

Definition 1.1. Let K be a number field and A/K be an abelian variety of dimension g. We let $\alpha(g) = 2^{10}g^3$ and define

$$b(A/K) = b([K:\mathbb{Q}], g, h(A)) = \left((14g)^{64g^2}[K:\mathbb{Q}]\max\left(h(A), \log[K:\mathbb{Q}], 1\right)^2\right)^{\alpha(g)},$$

where $h(A)$ is the stable Faltings height of A. We also set $b(A/K; d) = b(d[K:\mathbb{Q}], g, h(A))$.

*davide.lombardo@math.u-psud.fr

Our first result is the following explicit bound for the quantity ℓ_0 introduced above:

Theorem 1.2. *Let A/K be an abelian variety of dimension $g \geq 3$ and G_{ℓ^∞} be the image of the natural representation $\rho_{\ell^\infty} : \operatorname{Gal}\left(\overline{K}/K\right) \to \operatorname{Aut} T_\ell A$. Suppose that:*

1. $\operatorname{End}_{\overline{K}}(A) = \mathbb{Z}$;
2. *there exists a place v of K, of good reduction for A and with residue field of order q_v, such that the characteristic polynomial of the Frobenius at v (cf. section 2.3) has Galois group $(\mathbb{Z}/2\mathbb{Z})^g \rtimes S_g$.*

The equality $G_{\ell^\infty} = \operatorname{GSp}_{2g}(\mathbb{Z}_\ell)$ holds for every prime ℓ unramified in K and strictly larger than

$$\max\left\{ \left(2q_v^{4(\sqrt{6g}+1)}\right)^{2^g \cdot g!},\ b(A/K; g!),\ b(A^2/K; g)^{1/2g} \right\}.$$

Furthermore, the term $b(A^2/K; g)^{1/2g}$ can be omitted from the maximum if $g \geq 19$.

Remark 1.3. The cases $g = 1$ and $g = 2$ are treated in detail in [MW93b] (see also [Lom15]) and [Lom14] respectively.

Let us make a few comments on condition (2) in theorem 1.2. The hypothesis concerning the Galois group of $f_v(x)$ might seem somewhat unnatural, but it is a very simple way to encode the fact that the roots of $f_v(x)$ are "maximally generic"; in particular, this condition implies that the subgroup of $\overline{\mathbb{Q}}^\times$ they generate is free of rank $g + 1$, a fact which we will then use to prove modulo-ℓ analogues of the statement that the Zariski closure of G_{ℓ^∞} is of rank $g + 1$. We also remark that if at least one suitable place v exists, then such places have density one; furthermore, the existence of such a place is *equivalent* to the fact that the equality $G_{\ell^\infty} = \operatorname{GSp}_{2g}(\mathbb{Z}_\ell)$ holds for some ℓ. Thus, if the equality $G_{\ell^\infty} = \operatorname{GSp}_{2g}(\mathbb{Z}_\ell)$ holds for all sufficiently large primes ℓ (in particular, if the conclusion of the theorem is true for *some* bound $\ell_0(A/K)$), then it is very easy in practice to find a place v that satisfies condition (2), because such places have density one; see for example the explicit calculation of section 14 and the remarks preceding lemma 7.6. From a more theoretical perspective, we remark that a theorem of Pink (combined with previous work of Serre) implies that such places v always exist if the dimension of A lies outside a certain (very thin) set of "exceptional" dimensions; indeed, this is a consequence of the following result:

Theorem 1.4. *(Pink [Pin98], Serre [Ser86] [Ser00a]) Let A be an abelian variety of dimension g defined over the number field K, and let*

$$S = \left\{ \frac{1}{2}(2n)^k \mid n > 0, k \geq 3 \text{ odd} \right\} \cup \left\{ \frac{1}{2}\binom{2n}{n} \mid n > 1 \text{ odd} \right\}.$$

If $\operatorname{End}_{\overline{K}}(A) = \mathbb{Z}$ and $\dim A \notin S$, then:

- *the Mumford-Tate conjecture is true for A;*
- *the Mumford-Tate group of A is isomorphic to $\operatorname{GSp}_{2g,\mathbb{Q}}$;*
- *the equality $G_{\ell^\infty} = \operatorname{GSp}_{2g}(\mathbb{Z}_\ell)$ holds for every sufficiently large prime ℓ.*

Remark 1.5. The set S is precisely the set of those positive integers g such that there exists a symplectic minuscule representation of dimension $2g$ of a simple, simply connected algebraic group different from Sp_{2g}, cf. section 9.

In order to have a completely effective result we would also need to show that the number q_v above can be effectively bounded *a priori* in terms of simple arithmetical invariants of A/K. While unfortunately we cannot do this for arbitrary g, for simple abelian *threefolds* we prove:

Theorem 1.6. *(Theorem 12.17) Let A/K be an abelian variety of dimension 3 such that $\mathrm{End}_{\overline{K}}(A) = \mathbb{Z}$. Denote by $\mathcal{N}^0_{A/K}$ the naive conductor of A/K, that is, the product of the prime ideals of $\mathcal{O}_K$ at which A has bad reduction, and suppose that $A[7]$ is defined over K.*

- *Assume the Generalized Riemann Hypothesis: then the equality $G_{\ell^\infty} = \mathrm{GSp}_6(\mathbb{Z}_\ell)$ holds for every prime ℓ unramified in K and strictly larger than $(2q)^{48}$, where*
$$q = b(A^2/K;3)^8 \left(\log|\Delta_{K/\mathbb{Q}}| + \log N_{K/\mathbb{Q}}\left(\mathcal{N}^0_{A/K}\right)\right)^2.$$
- *Unconditionally, the same conclusion holds with*
$$q = \exp\left(cb(A^2/K;3)^8 \left(\log|\Delta_K| + \log N_{K/\mathbb{Q}}\left(\mathcal{N}^0_{A/K}\right)\right)^2\right),$$
where c is an absolute effectively computable constant.

Remark 1.7. The condition that the 7-torsion points of A are defined over K is not very restrictive, for it can be met by simply replacing K by $K(A[7])$, cf. remark 12.18.

Remark 1.8. Unpublished work of Winckler [Win] shows that c can be taken to be 27175010, see also the recent preprint [Zam15]. Furthermore, if A/K is a semistable abelian variety, then $\log N_{K/\mathbb{Q}}\left(\mathcal{N}^0_{A/K}\right)$ is bounded above by $[K:\mathbb{Q}]\,(c_0h(A)+c_1)$ for certain constants c_0, c_1 depending only on $[K:\mathbb{Q}]$ and on $\dim A$: this result is stated and proved in [HP15] (see especially Theorem 6.5 of *op. cit.*) for abelian varieties over function fields, but the same proof works equally well also over number fields (for a detailed proof in the number field case see also [Paz15, Theorem 1.1]).

When the dimension of A grows, the complexity of the problem of computing a bound $\ell_0(A/K)$ increases as well, and (at least with the techniques developed in this paper) it becomes extremely impractical to give completely explicit results. Even in these higher-dimensional situations, however, our methods are not entirely powerless, and as an example of possible further extensions we show:

Theorem 1.9. *Let A/K be an abelian variety of dimension 5 such that $\mathrm{End}_{\overline{K}}(A) = \mathbb{Z}$. There is an effective bound $\ell_0(A/K)$ (depending on $h(A)$, on the discriminant Δ_K of K, and on $\mathcal{N}^0_{A/K}$) such that $G_{\ell^\infty} = \mathrm{GSp}_{10}(\mathbb{Z}_\ell)$ for every $\ell > \ell_0(A/K)$.*

Remark 1.10. No such result can exist in dimension 4, since it is known by work of Mumford [Mum69] that there exist simple abelian fourfolds A/K with geometrically trivial endomorphism ring (i.e. $\mathrm{End}_{\overline{K}}(A) = \mathbb{Z}$) such that the Zariski closure of G_{ℓ^∞} is of rank 4 for every prime ℓ. Since the rank of $\mathrm{GSp}_{8,\mathbb{Q}_\ell}$ is 5, this shows that for such fourfolds we can never have $G_{\ell^\infty} = \mathrm{GSp}_8(\mathbb{Z}_\ell)$ – in particular, hypothesis (2) of theorem 1.2 does not hold for such A.

To conclude this introduction we now describe the organization of this paper. After two sections of preliminaries (§ 2 and 3) we study the various classes of maximal proper subgroups G of $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$, showing that – at least for ℓ large enough – G_ℓ cannot be contained in any such G. This occupies sections 4 through 10, each of which deals with a different kind of maximal subgroup. Next in §11 we prove theorem 1.2, while section 12 contains a proof of theorem 1.6. In section 13 we further extend the techniques of §12 to prove theorem 1.9. Finally, section 14 contains an example of an abelian threefold for which theorem 1.2 enables us to establish explicit surjectivity results, and to which previously available methods seem not to be applicable.

We say a few more words on the techniques used in sections 4 through 10. Three classes of maximal subgroups (traditionally dubbed "imprimitive", "reducible", and "field extension" cases) are dealt with in section 4 as an almost immediate consequence of the isogeny theorem of Masser and Wüstholz [MW93a] [MW93c] (the completely explicit version we employ is due to Gaudron and Rémond [GR14]). Other maximal subgroups of $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$ are closely related to the image of the $2g$-dimensional symplectic representation of $\mathrm{PGL}_2(\mathbb{F}_\ell)$, and in section 5 we show that, for ℓ sufficiently large, G_ℓ cannot be contained in such a subgroup: this is obtained by comparing purely group-theoretical information with Raynaud's description of the structure of $A[\ell]$ as a module over the inertia group at a place of characteristic ℓ. If we assume A to be semistable, this result is essentially uniform in the abelian variety; however, we also give a non-uniform bound, based on the properties of the place v, which allows us to avoid the need for a semistability assumption in the hypotheses of theorem 1.2. The uniform bounds, on the other hand, are certainly interesting in themselves, and they will also be used to establish theorem 1.6.

The aforementioned results of Raynaud are also used in section 6 to eliminate the possibility of G_ℓ being a small "exceptional" (or "constant") group: we obtain a lower bound on $|\mathbb{P}G_\ell|$ that is linear in ℓ (and essentially uniform in A), which – combined with results of Larsen-Pink and Collins – shows that the exceptional case does not arise for ℓ larger than a certain explicit function of g. As in the previous case, this result depends on a semistability assumption, and we complement it with an unconditional (but non-uniform) bound based on the isogeny theorem.

In §7 and §8 we consider the case of G_ℓ being contained in a "tensor product" subgroup, and we show how, given a place v as in hypothesis (2) of theorem 1.2, one can produce a finite set of integers whose divisors include all the primes for which G_ℓ is of tensor product type; this is inspired by an argument of Serre [Ser00a], but his use of the characteristic polynomial of Fr_v is almost completely replaced by a direct study of the multiplicative relations satisfied by its roots. These relations also form the main object of interest in §12, where we exploit their simple form and the manageable structure of the subgroups of $\mathrm{GO}_3(\mathbb{F}_\ell)$ to show how, if $\dim A = 3$, a careful application of Chebotarev's theorem yields an effective bound on the residual characteristic of a place v with the desired properties. Finally, in sections 9 and 10 we use tools from representation theory (of both algebraic and finite groups) to treat the last remaining classes of maximal subgroups of $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$, namely the so-called subgroups of class $\mathcal{S}$ and the tensor-induced ("class $\mathcal{C}_7$") subgroups. Roughly speaking, representation theory is used to show that if G_ℓ is contained in a group of class $\mathcal{S}$ or of class $\mathcal{C}_7$, then the eigenvalues of every Frobenius element of K (when reduced modulo ℓ) satisfy a certain polynomial equation with small exponents; once this has been established, the proof proceeds along the same general lines as in section 7.

Acknowledgments. I thank N. Ratazzi for suggesting the problem and J.-P. Serre for inspiring discussions.

2 Preliminaries

2.1 The isogeny theorem

The result that makes many of the explicit estimates possible is the following theorem, originally due to Masser and Wüstholz [MW93c] [MW93a] and then improved and made explicit by Gaudron and Rémond [GR14]:

Theorem 2.1. *(Isogeny Theorem, [GR14, Theorem 1.4]) Let A/K be an abelian variety. For every abelian variety A^* defined over K that is K-isogenous to A, there exists a K-isogeny $A^* \to A$ whose degree is bounded by $b(A/K)$ (cf. definition 1.1).*

It is very likely that the function $b(A/K)$ of definition 1.1 is not the best possible one. Let us then introduce another function $b_0(A/K)$, which is by definition the optimal isogeny bound:

Definition 2.2. Let A/K be an abelian variety. We denote by $b_0(A/K)$ the smallest natural number such that, for every other abelian variety B/K that is K-isogenous to A, there exists a K-isogeny $B \to A$ of degree at most $b_0(A/K)$. We set $b_0(A/K; d) = \max_{[K':K]\leq d} b_0(A/K')$, where the maximum is taken over the finite extensions of K of degree at most d.

It is clear that the isogeny theorem implies that $b_0(A/K)$ and $b_0(A/K;d)$ exist, and that $b_0(A/K;d) \leq b(d[K:\mathbb{Q}], \dim A, h(A)) = b(A/K;d)$. Whenever possible, we will state our results in terms of b_0 instead of b; in some situations, however, in order to avoid cumbersome expressions involving maxima we simply give bounds in terms of the function b.

2.2 Weil pairing, Serre's lifting lemma

Let $A^\vee$ be the dual variety of A and let $\langle\cdot,\cdot\rangle$ denote the Weil pairing on $A\times A^\vee$. Also let $\mathbb{Z}_\ell(1)$ be the 1-dimensional Galois module the action on which is given by the cyclotomic character $\chi_\ell : \operatorname{Gal}\left(\overline{K}/K\right) \to \mathbb{Z}_\ell^\times$. For any choice of a polarization $\varphi : A \to A^\vee$, the composition

$$T_\ell(A) \times T_\ell(A) \xrightarrow{\operatorname{id}\times\varphi} T_\ell(A) \times T_\ell(A^\vee) \xrightarrow{\langle\cdot,\cdot\rangle} \mathbb{Z}_\ell(1)$$

equips the Tate module $T_\ell(A)$ with a Galois-equivariant, skew-symmetric form which we still denote by $\langle\cdot,\cdot\rangle$ and call the Weil pairing on $T_\ell(A)$. By Galois-equivariance of $\langle\cdot,\cdot\rangle$, every element h of the group G_{ℓ^∞} preserves the form $\langle\cdot,\cdot\rangle$ up to multiplication by a scalar factor (called the *multiplier* of h), so G_{ℓ^∞} is in fact contained in $\operatorname{GSp}(T_\ell(A)\otimes_{\mathbb{Z}_\ell}\mathbb{Q}_\ell, \langle\cdot,\cdot\rangle)$, the group of symplectic similitudes of $T_\ell(A)\otimes_{\mathbb{Z}_\ell}\mathbb{Q}_\ell$ with respect to $\langle\cdot,\cdot\rangle$. Notice that the multiplier of h need not be an ℓ-adic unit, whence the need to tensor by $\mathbb{Q}_\ell$. Suppose however that ℓ does not divide the degree of the polarization φ: then $\operatorname{id}\times\varphi$ induces an isomorphism between $T_\ell(A)\times T_\ell(A)$ and $T_\ell(A)\times T_\ell(A^\vee)$, from which one easily deduces that the multiplier of every $h \in G_{\ell^\infty}$ is an ℓ-adic unit. It follows that (for these primes) G_{ℓ^∞} is a subgroup of $\operatorname{GSp}(T_\ell(A), \langle\cdot,\cdot\rangle)$, so, after a choice of basis, we can consider G_{ℓ^∞} as being a subgroup of $\operatorname{GSp}_{2g}(\mathbb{Z}_\ell)$.

Fix now (once and for all) a polarization φ of A of minimal degree. By [GR14, Théorème 1.1] we see that $\deg \varphi \leq b(A/K)$, so (since we only work with primes strictly larger than this quantity) we can assume that G_{ℓ^∞} is a subgroup of $\operatorname{GSp}_{2g}(\mathbb{Z}_\ell)$. Moreover, for such values of ℓ the Weil pairing is nondegenerate on $A[\ell]$, so for all primes $\ell > b(A/K)$ the group G_ℓ is a subgroup of $\operatorname{GSp}_{2g}(\mathbb{F}_\ell)$. Combining this remark with the following well-known lemma, originally due to Serre, will allow us to only consider the residual mod-ℓ representation ρ_ℓ instead of the full ℓ-adic system ρ_{ℓ^∞}:

Lemma 2.3. *Let g be a positive integer, $\ell \geq 5$ be a prime and G be a closed subgroup of $\operatorname{Sp}_{2g}(\mathbb{Z}_\ell)$. Suppose that G surjects onto $\operatorname{Sp}_{2g}(\mathbb{F}_\ell)$ by reduction modulo ℓ: then $G = \operatorname{Sp}_{2g}(\mathbb{Z}_\ell)$. Likewise, let H be a closed subgroup of $\operatorname{GSp}_{2g}(\mathbb{Z}_\ell)$ whose reduction modulo ℓ contains $\operatorname{Sp}_{2g}(\mathbb{F}_\ell)$: then $H' = \operatorname{Sp}_{2g}(\mathbb{Z}_\ell)$.*

Proof. The first statement is [Ser00a, Lemma 1 on p. 52], cf. also Theorem 1.3 in [Vas03]. The second part follows by applying the first to $G = H'$ and noticing that the reduction modulo ℓ of H' contains the derived subgroup of $\operatorname{Sp}_{2g}(\mathbb{F}_\ell)$ which, for $\ell \geq 5$, is $\operatorname{Sp}_{2g}(\mathbb{F}_\ell)$ itself. $\square$

Corollary 2.4. *Let $\ell > b(A/K)$: then G_ℓ is contained in $\operatorname{GSp}_{2g}(\mathbb{F}_\ell)$. Suppose ℓ does not ramify in K: then $\operatorname{Gal}\left(\overline{K}/K\right) \xrightarrow{\chi_\ell} \mathbb{Z}_\ell^\times$ is surjective. In particular, if $\ell > b(A/K)$ does not ramify in K, the inclusion $\operatorname{Sp}_{2g}(\mathbb{F}_\ell) \subseteq G_\ell$ implies $G_{\ell^\infty} = \operatorname{GSp}_{2g}(\mathbb{Z}_\ell)$.*

We conclude this section by recording for future reference our working assumption that ℓ does not divide the degree of a minimal polarization. This is a minor technical point, but is nonetheless necessary if we want our statements (which often involve the group $\operatorname{GSp}_{2g}(\mathbb{F}_\ell)$) to be meaningful.

Assumption 2.5. The prime ℓ does not divide the degree of a minimal polarization of A. In particular, this allows us to identify G_ℓ (resp. G_{ℓ^∞}) to a subgroup of $\operatorname{GSp}_{2g}(\mathbb{F}_\ell)$ (resp. $\operatorname{GSp}_{2g}(\mathbb{Z}_\ell)$).

2.3 Frobenius elements and their eigenvalues

We conclude this section of preliminaries by introducing our notation for Frobenius elements and their eigenvalues, and by proving some simple facts about them. We let Ω_K denote the set of finite places of K, and for each $v \in \Omega_K$ we write p_v for the residual characteristic and q_v for the cardinality of the residue field at v. We also write $\operatorname{Fr}_v \in \operatorname{Gal}\left(\overline{K}/K\right)$ for a Frobenius element at v. If v is a place of K of good reduction for A, the characteristic polynomial of $\rho_{\ell^\infty}(\operatorname{Fr}_v)$ does not depend on ℓ (as long as $v \nmid \ell$), and will be denoted by $f_v(x) \in \mathbb{Z}[x]$. We shall write $\mu_1, \ldots, \mu_{2g}$ for the roots of $f_v(x)$ in $\overline{\mathbb{Q}}$, and call these algebraic integers the **eigenvalues of** Fr_v.

The splitting field of $f_v(x)$ is a Galois extension of $\mathbb{Q}$ which we call $F(v)$. Recall that, thanks to the Weil conjectures, the absolute value of every μ_i under any embedding of $F(v)$ in $\mathbb{C}$ is equal to $q_v^{1/2}$. If ℓ is a prime not lying below v, let $\mathfrak{l}$ be any prime of $F(v)$ lying above ℓ, and let $\mathbb{F}_\mathfrak{l}$ be the residue field at $\mathfrak{l}$. Since the μ_i's are algebraic *integers*, it makes sense to consider their reductions modulo $\mathfrak{l}$: they are elements of $\overline{\mathbb{F}_\ell}^\times$ which we will denote by $\overline{\mu_1}, \ldots, \overline{\mu_{2g}}$, and which can also be identified with the roots in $\overline{\mathbb{F}_\ell}$ of the characteristic polynomial of $\rho_\ell(\operatorname{Fr}_v)$. When speaking of the roots $\overline{\mu_1}, \ldots, \overline{\mu_{2g}}$ of the characteristic polynomial of $\rho_\ell(\operatorname{Fr}_v)$ we shall always implicitly assume that this identification has been made.

Definition 2.6. To avoid confusion between the notation $\overline{\mu_i}$ (the reduction of μ_i in $\overline{\mathbb{F}_\ell}$) and the complex conjugate of μ_i, we shall denote the latter by $\iota(\mu_i)$. We also denote by Φ_v the set of roots of $f_v(x)$.

Lemma 2.7. *The splitting field $F(v)$ of the characteristic polynomial $f_v(x)$ of* Fr_v *has Galois group isomorphic to a subgroup of $(\mathbb{Z}/2\mathbb{Z})^g \rtimes S_g$, so it has degree at most $2^g g!$ over $\mathbb{Q}$.*

Proof. Immediate from the relation $x^{2g} f_v\left(q_v x^{-1}\right) = q_v^g f_v(x)$, which in turn follows from $\rho_{\ell^\infty}(\mathrm{Fr}_v)$ being an element of $\mathrm{GSp}_{2g}(\mathbb{Z}_\ell)$ for any sufficiently large prime ℓ and from the Weil conjectures. □

Essentially by the same argument as in the previous lemma, it is easy to see that the subgroup of $\overline{\mathbb{Q}}^\times$ generated by the eigenvalues of a Frobenius element Fr_v has rank at most $g+1$, and we are interested in places v for which equality is attained. We shall now concentrate on those Frobenius elements that are "maximally generic" in the following sense: we consider places v such that the the Galois group of the characteristic polynomial $f_v(x)$ is the full Weyl group $\mathcal{W}_g := (\mathbb{Z}/2\mathbb{Z})^g \rtimes S_g$. In this case, we shall now see that the group generated by the eigenvalues of Fr_v is free of rank $g+1$ (corollary 2.10). We also collect here various "multiplicative independence" results that will be used repeatedly throughout the paper.

Lemma 2.8. *Suppose $g = \dim A$ is at least 3. Suppose $f_v(x)$ has Galois group isomorphic to $(\mathbb{Z}/2\mathbb{Z})^g \rtimes S_g$ and order the roots $\mu_1, \ldots, \mu_{2g}$ of $f_v(x)$ in such a way that $\iota(\mu_i) = \mu_{2g+1-i}$. Let $(n_1, \ldots, n_{2g}) \in \mathbb{Z}^{2g}$ be such that $\displaystyle\prod_{i=1}^{2g} \mu_i^{n_i}$ is a real number: then for all $i = 1, \ldots, 2g$ we have $n_i = n_{2g+1-i}$.*

Proof. The number $\prod_{i=g+1}^{2g} (\mu_i \mu_{2g+1-i})^{-n_i} = \prod_{i=g+1}^{2g} q_v^{-n_i}$ is in $\mathbb{R}$, so the product

$$\prod_{i=1}^{2g} \mu_i^{n_i} \prod_{i=g+1}^{2g} (\mu_i \mu_{2g+1-i})^{-n_i} = \prod_{i=1}^{g} \mu_i^{n_i - n_{i+g}}$$

is again a real number. We can therefore assume that we have $n_j = 0$ for $j = g+1, \ldots, 2g$, in which case our claim becomes the statement that $n_i = 0$ for $i = 1, \ldots, g$. Suppose this is not the case, and let $k \in \{1, \ldots, g\}$ be an index such that $n_k \neq 0$. Let σ be the element of $\mathrm{Gal}(F(v)/\mathbb{Q})$ that exchanges μ_k with $\mu_{2g+1-k} = \iota(\mu_k)$ while fixing μ_j for $j = 1, \ldots, g, j \neq i$. Now notice that

$$\left| \prod_{i=1}^{g} \mu_i^{n_i} \right| = \prod_{i=1}^{g} |\mu_i|^{n_i} = \sqrt{q_v}^{\sum_{i=1}^g n_i},$$

so $\prod_{i=1}^{g} \mu_i^{2n_i} = q_v^{\sum_{i=1}^g n_i}$ is a rational number. Thus we have

$$\prod_{i \neq k} \mu_i^{2n_i} \cdot \iota(\mu_k)^{2n_k} = \sigma \left(\prod_{i=1}^{g} \mu_i^{2n_i} \right) = \prod_{i=1}^{g} \mu_i^{2n_i} \Rightarrow (\mu_k/\iota(\mu_k))^{2n_k} = 1.$$

But this implies $\iota(\mu_k)^{4n_k} = (\mu_k \iota(\mu_k))^{2n_k} = q_v^{2n_k}$, so the Galois group of the minimal polynomial of $\iota(\mu_k)$ embeds in the Galois group of $x^{4n_k} - q_v^{2n_k}$. The latter is either the cyclic group $\mathbb{Z}/2n_k\mathbb{Z}$ or the dihedral group D_{2n_k} (depending on whether or not q_v is a square in $\mathbb{Q}$), while the former is by assumption isomorphic to $(\mathbb{Z}/2\mathbb{Z})^g \rtimes S_g$. This immediately leads to a

contradiction if $g \geq 5$, because the Galois group of $x^{4n_k} - q_v^{2n_k}$ is solvable while $(\mathbb{Z}/2\mathbb{Z})^g \rtimes S_g$ is not. For $g = 3$ or 4 notice that the derived length (that is, the length of the derived series) of the solvable group D_{2n_k} is 2, while the derived length of $(\mathbb{Z}/2\mathbb{Z})^g \rtimes S_g$ is at least 3, which gives a contradiction also in the case $g \in \{3, 4\}$. $\square$

Notice that in the course of the proof we have also established:

Lemma 2.9. *Suppose* $\dim A \geq 3$. *Let v be a place of K at which A has good reduction, and suppose that $f_v(x)$ has Galois group $(\mathbb{Z}/2\mathbb{Z})^g \rtimes S_g$: then for every positive integer m the polynomials $f_v(x)$ and $h_\pm(x) = x^{2m} \pm q_v^m$ have no common root.*

Corollary 2.10. *Suppose $g \geq 3$ and $f_v(x)$ has Galois group isomorphic to $(\mathbb{Z}/2\mathbb{Z})^g \rtimes S_g$. Order the roots $\mu_1, \ldots, \mu_{2g}$ of $f_v(x)$ in such a way that $\iota(\mu_i) = \mu_{2g+1-i}$. The abelian subgroup of $\overline{\mathbb{Q}}^\times$ generated by $\mu_1, \ldots, \mu_g, \mu_{g+1}, \ldots, \mu_{2g}$ is free of rank $g+1$. We can take as generators $\mu_1, \ldots, \mu_g, \mu_{g+1}$.*

Proof. Since $\mu_g\mu_{g+1} = \mu_i\mu_{2g+1-i}$ for all $i = 1, \ldots, g$, it is clear that the group generated by $\mu_1, \ldots, \mu_{2g}$ is the same as the group generated by $\mu_1, \ldots, \mu_g, \mu_{g+1}$. Thus it suffices to show that $\mu_1^{n_1} \cdots \mu_g^{n_g} \mu_{g+1}^{n_{g+1}} = 1$ implies $n_1 = \cdots = n_g = n_{g+1} = 0$. By lemma 2.8, the equality $\mu_1^{n_1} \cdots \mu_g^{n_g} \mu_{g+1}^{n_{g+1}} = 1$ immediately implies $n_2 = \cdots = n_g = 0$ and $n_1 = n_{g+1}$. Taking absolute values in the equality $\mu_1^{n_1} \cdots \mu_g^{n_g} \mu_{g+1}^{n_{g+1}} = 1$ we then find $q_v^{n_1} = 1$, that is, $n_1 = 0$. $\square$

Corollary 2.11. *With the notation and the hypotheses of lemma 2.8, let n be an odd integer and N be any positive integer. For all injective functions $j : \{1, 2, \ldots, 2n\} \longrightarrow \{1, \ldots, 2g\}$ we have*

$$\prod_{i=1}^{n} \mu_{j(i)}^N \neq \prod_{i=n+1}^{2n} \mu_{j(i)}^N$$

Proof. Suppose by contradiction $\prod_{i=1}^{n} \mu_{j(i)}^N \prod_{i=n+1}^{2n} \mu_{j(i)}^{-N} = 1$. By lemma 2.8 the number of variables with exponent equal to N, that is n, is even, but this contradicts the assumption. $\square$

Lemma 2.12. *With the notation and the hypotheses of lemma 2.8, let λ, ν_1, ν_2 be three distinct eigenvalues of* Fr_v. *We have $\lambda^2 \neq \nu_1\nu_2$.*

Proof. Suppose by contradiction that $\lambda^2 = \nu_1\nu_2$. The action of $\mathcal{W}_g$ on the set $\{\mu_1, \ldots, \mu_{2g}\}$ has the following property: for every $\sigma \in \mathcal{W}_g$ and for every pair of indices i, j, we have $\sigma(\mu_i) = \mu_j$ if and only if $\sigma(\mu_{2g+1-i}) = \mu_{2g+1-j}$. Suppose first that $\nu_2 \notin \{\iota(\nu_1), \iota(\lambda)\}$: then there exists a $\sigma \in \mathcal{W}_g$ which fixes both ν_1 and λ, but such that $\sigma(\nu_2) \neq \nu_2$. Applying σ to the equality $\lambda^2 = \nu_1\nu_2$ we find $\lambda^2 = \nu_1\sigma(\nu_2)$, which is a contradiction since $\sigma(\nu_2) \neq \nu_2$. Next suppose that $\nu_2 = \iota(\lambda)$: then $\iota(\nu_1)$ is different from λ and from ν_2 (since λ, ν_1, ν_2 are all distinct), and we can just repeat the same argument with ν_2 replaced by ν_1. Finally, assume ν_1, ν_2 are complex conjugates of each other (hence they are both distinct from λ and $\iota(\lambda)$), and denote by S the stabilizer of ν_1, ν_2 in $\mathcal{W}_g$: since $g \geq 3$, the orbit of λ under the action of S has order at least 4, hence in particular there is a $\sigma \in S$ such that $\sigma(\lambda) \neq \pm\lambda$. Applying this σ to the equation $\lambda^2 = \nu_1\nu_2$ leads once more to a contradiction. $\square$

Lemma 2.13. *With the notation and the hypotheses of lemma 2.8, let $\lambda_1, \lambda_2, \lambda_3, \lambda_4$ be four distinct eigenvalues of* Fr_v. *The equality $\lambda_1\lambda_2 = \lambda_3\lambda_4$ implies $\lambda_2 = \iota(\lambda_1)$ and $\lambda_4 = \iota(\lambda_3)$.*

Proof. Consider the stabilizer of $\lambda_1, \lambda_2, \lambda_3$ in $\mathrm{Gal}\,(F(v)/\mathbb{Q})$, and let σ be any element of this stabilizer. Applying σ to the equation $\lambda_1\lambda_2 = \lambda_3\lambda_4$ we find $\sigma(\lambda_4) = \lambda_4$, that is, the stabilizer of $\lambda_1, \lambda_2, \lambda_3$ fixes λ_4. Given the structure of $\mathrm{Gal}\,(F(v)/\mathbb{Q})$ (which is by assumption isomorphic to $(\mathbb{Z}/2\mathbb{Z})^g \rtimes S_g$), this is only possible if $\iota(\lambda_4) \in \{\lambda_1, \lambda_2, \lambda_3\}$. Assume by contradiction that $\iota(\lambda_4) \in \{\lambda_1, \lambda_2\}$; then by symmetry we can assume $\lambda_4 = \iota(\lambda_1)$. The same argument then also shows that $\lambda_3 = \iota(\lambda_2)$, so our original equation rewrites as

$$\lambda_1\lambda_2 = \iota(\lambda_1\lambda_2). \tag{1}$$

Let now $\tau \in \mathrm{Gal}(F(v)/\mathbb{Q})$ be an operator that exchanges $\lambda_1, \iota(\lambda_1)$ while fixing $\lambda_2, \iota(\lambda_2)$; such an operator clearly exists in $(\mathbb{Z}/2\mathbb{Z})^g \rtimes S_g$. Applying this τ to equation (1) we find $\lambda_1\iota(\lambda_2) = \iota(\lambda_1)\lambda_2$, which together with (1) implies $\iota(\lambda_2^2) = \lambda_2^2$, that is, λ_2^2 is in $\mathbb{R}$. On the other hand, we know that $|\lambda_2| = q_v^{1/2}$ under any embedding of $F(v)$ in $\mathbb{C}$, hence we must have $\lambda_2^2 = \pm q_v$. However, this contradicts the fact that λ_2 has degree $2g$ over $\mathbb{Q}$, hence we cannot have $\iota(\lambda_4) \in \{\lambda_1, \lambda_2\}$. It follows that $\lambda_4 = \iota(\lambda_3)$ and $\lambda_3\lambda_4 = q_v \in \mathbb{Q}$, so $\lambda_1\lambda_2$ is fixed under the action of $\mathrm{Gal}(F(v)/\mathbb{Q})$; by the same argument as above, this is only possible if $\lambda_2 = \iota(\lambda_1)$, and we are done. $\square$

Lemma 2.14. *Suppose $g = \dim A$ is at least 3 and $f_v(x)$ has Galois group isomorphic to $(\mathbb{Z}/2\mathbb{Z})^g \rtimes S_g$. Let Φ_v be the set of roots of $f_v(x)$.*

- *Let $f_1 : \Phi_v^{2g} \to \mathbb{N}$ be given by*

  $$f_1(x_1, \ldots, x_{2g}) = |N_{F(v)/\mathbb{Q}}(x_1x_3 - x_2x_4)| + |N_{F(v)/\mathbb{Q}}(x_1x_6 - x_2x_5)|$$

  If $(x_1, \ldots, x_{2g}) \in \Phi_v^{2g}$ are all distinct, then we have $0 \neq f_1(x_1, \ldots, x_{2g}) \leq 2(2q_v)^{[F(v):\mathbb{Q}]}$.

- *Likewise, let $f_2 : \Phi_v^{2g} \to \mathbb{N}$ be given by $f_2(x_1, \ldots, x_{2g}) = |N_{F(v)/\mathbb{Q}}(x_2^2 - x_1x_3)|$. If $(x_1, \ldots, x_{2g}) \in \Phi_v^{2g}$ are all distinct, then we have $0 \neq f_2(x_1, \ldots, x_{2g}) \leq (2q_v)^{[F(v):\mathbb{Q}]}$.*

Proof. It is clear by construction that $f_1(x_1, \ldots, x_{2g})$ is the sum of two non-negative integers. Furthermore, the Weil conjectures imply that the inequality

$$|\sigma(x_ix_j - x_kx_l)| \leq |\sigma(x_ix_j)| + |\sigma(x_kx_l)| \leq 2q_v$$

holds for every choice of indices i, j, k, l and of $\sigma \in \mathrm{Gal}(F(v)/\mathbb{Q})$, so each summand in the definition of f_1 does not exceed $(2q_v)^{[F(v):\mathbb{Q}]}$. This proves the second inequality in the statement. To prove the first, it suffices to show that the two summands cannot vanish at the same time. This follows easily from lemma 2.13. Assume that $\left|N_{F(v)/\mathbb{Q}}(x_1x_3 - x_2x_4)\right|$ is zero: then $x_1x_3 - x_2x_4$ itself is zero, and by lemma 2.13 we must have $x_3 = \iota(x_1)$. If by contradiction $|N_{F(v)/\mathbb{Q}}(x_1x_6 - x_2x_5)|$ also vanished, then by the same argument we would have $x_6 = \iota(x_1) = x_3$, contradicting the hypothesis that the x_i are all distinct.

As for the second statement, the inequality $f_2(x_1, \ldots, x_{2g}) \leq (2q_v)^{[F(v):\mathbb{Q}]}$ follows again from the Weil conjectures, while the inequality $f_2(x_1, \ldots, x_{2g}) \neq 0$ has already been shown in the course of the proof of lemma 2.12. $\square$

3 Maximal subgroups of $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$

Thanks to corollary 2.4 we see that in order to prove theorem 1.2 it is enough to show that the equality $G_\ell = \mathrm{GSp}_{2g}(\mathbb{F}_\ell)$ holds all ℓ larger than a certain explicit bound. In order to do this, we shall make use of a description of the maximal proper subgroups of $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$: the core of our argument will consist in showing that – for ℓ large enough – G_ℓ cannot be contained in any proper subgroup of $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$, and hence it has to coincide with all of $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$. The purpose of this section is to introduce some notation and state theorem 3.14, which gives precisely such a classification of the maximal subgroups of $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$. Our main references for this section are [BHRD13] and [KL90].

3.1 Group theoretical preliminaries

We now recall some basic facts from finite group theory that will be needed in what follows.

Definition 3.1. Let G be a finite group. The **socle** of G, denoted $\mathrm{soc}(G)$, is the subgroup of G generated by the non-trivial minimal normal subgroups of G.

Definition 3.2. A finite group G is said to be **almost simple** if its socle is a non-abelian simple group. In this case, if we let $S = \mathrm{soc}(G)$, we have $S \leq G \leq \mathrm{Aut}(S)$, and S is a normal subgroup of G.

Lemma 3.3. *An almost simple group G does not possess non-trivial normal solvable subgroups.*

Proof. Suppose a nontrivial normal solvable subgroup exists. Then the collection of such subgroups is nonempty, and there is a minimal normal subgroup N_0 of G that is solvable (a subgroup of a solvable group is itself solvable). The definition of $\mathrm{soc}(G)$ implies $N_0 \subset \mathrm{soc}(G)$, and moreover N_0 is normal in $\mathrm{soc}(G)$ since it is normal in G. By simplicity of $\mathrm{soc}(G)$ this forces $N_0 = \mathrm{soc}(G)$; however, the latter is simple non-abelian, hence in particular not solvable, contradiction. $\square$

Lemma 3.4. *An almost-simple group G has a unique non-trivial minimal normal subgroup, which coincides with its socle.*

Proof. Let N be a non-trivial minimal normal subgroup of G. We have $N \triangleleft \mathrm{soc}(G)$, and as the latter is simple this forces $N = \mathrm{soc}(G)$. $\square$

Definition 3.5. Let S be a finite group. The group $\mathrm{Inn}(S)$ of **inner automorphisms** of S is the image of the map

$$\begin{array}{ccc} S & \to & \mathrm{Aut}(S) \\ g & \mapsto & \left(\begin{array}{cccc} \varphi_g : & S & \to & S \\ & s & \mapsto & gsg^{-1} \end{array} \right). \end{array}$$

The group $\mathrm{Inn}(S)$ is a normal subgroup of $\mathrm{Aut}(S)$. The quotient $\mathrm{Aut}(S)/\mathrm{Inn}(S)$ is called the **group of outer automorphisms** of G, and is denoted by $\mathrm{Out}(S)$.

Definition 3.6. A group is said to be **perfect** if it equals its commutator subgroup. If H is a finite group we denote by H^∞ the first perfect group contained in the derived series of H; equivalently,

$$H^\infty = \bigcap_{i \geq 0} H^{(i)},$$

where $H^{(0)} = H$ and $H^{(i+1)} = [H^{(i)}, H^{(i)}]$.

Lemma 3.7. *If G is almost simple we have $\operatorname{soc}(G) = G^\infty$; in particular, $\operatorname{soc}(G)$ is perfect.*

Proof. This follows immediately from the fact that the outer automorphism group of a simple group is solvable ([BHRD13, Theorem 1.3.2]). □

3.2 Definition of the classical groups

We now recall various standard constructions that are frequently used in the theory of finite matrix groups. Let F be a finite field of characteristic different from 2 and n be an odd integer. The **group of orthogonal transformations** of F^n is

$$\mathrm{GO}_n(F) = \left\{ x \in \mathrm{GL}_n(F) \;\middle|\; x^t x = \mathrm{Id} \right\};$$

we also define the **special orthogonal group** $\mathrm{SO}_n(F) = \left\{ x \in \mathrm{GO}_n(F) \;\middle|\; \det x = 1 \right\}$ and the **group of orthogonal similarities**

$$\mathrm{CGO}_n(F) = \left\{ x \in \mathrm{GL}_n(F) \;\middle|\; \exists \lambda \in F^\times \text{ such that } x^t x = \lambda \, \mathrm{Id} \right\}.$$

We shall also need to consider the groups $\Omega_n(F)$:

Definition 3.8. ([BHRD13, p. 29]) Let $n \geq 3$ be odd: the group $\Omega_n(F)$ is the unique subgroup of $\mathrm{SO}_n(F)$ of index 2.

Remark 3.9. The group $\Omega_n(F)$ is usually introduced as the kernel of the so-called spinor norm $\mathrm{SO}_n(\mathbb{F}_\ell) \to \{\pm 1\}$; the precise definition of the spinor norm, however, is somewhat convoluted, while the simpler definition 3.8 is perfectly suitable for our purposes. Also notice that for any finite field F of odd characteristic the groups $\mathbb{P}\Omega_3(F)$ and $\mathrm{PSL}_2(F)$ are isomorphic, cf. [BHRD13, Proposition 1.10.1] (here $\mathbb{P}\Omega_3(F)$ denotes the image of $\Omega_3(F)$ in $\mathrm{PGL}_3(F)$)

Suppose now that n is even (and $\operatorname{char} F \neq 2$). In this case there are precisely two isomorphism classes of isometry groups of symmetric bilinear forms ([BHRD13, §1.5]); we take standard representatives for these isomorphism classes as follows:

Definition 3.10. We let M^+ be the anti-diagonal matrix $\operatorname{antidiag}(1, \ldots, 1)$ of size n. Furthermore, we fix a generator ω_F of the multiplicative group $F^\times$, and let M^- be the diagonal matrix $\operatorname{diag}(\omega_F, 1, \ldots, 1)$ of size n. We then define the orthogonal groups

$$\mathrm{GO}_n^\pm(F) = \left\{ x \in \mathrm{GL}_n(F) \;\middle|\; x^t M^\pm x = M^\pm \right\}$$

and the corresponding groups of similarities

$$\mathrm{CGO}_n^\pm(F) = \left\{ x \in \mathrm{GL}_n(F) \;\middle|\; \exists \lambda \in F^\times \text{ such that } x^t M^\pm x = \lambda M^\pm \right\}.$$

We now introduce the symplectic groups. Let n be any positive integer. The **standard symplectic form** on F^{2n} is

$$\begin{array}{rccc} \langle\cdot,\cdot\rangle : & F^{2n}\times F^{2n} & \to & F \\ & (v,w) & \mapsto & v^tJw, \end{array}$$

where $J := \operatorname{antidiag}(\underbrace{1,\dots,1}_{n},\underbrace{-1,\dots,-1}_{n})$. We can then introduce the **group of symplectic transformations**,

$$\operatorname{Sp}_{2n}(F) = \left\{x\in \operatorname{GL}_{2n}(F) \;\middle|\; x^tJx = J\right\},$$

and the **group of symplectic similarities**

$$\operatorname{GSp}_{2n}(F) = \left\{x\in \operatorname{GL}_{2n}(F) \;\middle|\; \exists\lambda\in F^\times \text{ such that } x^tJx = \lambda J\right\}.$$

Let V_1, V_2 be two vector spaces over F. The **Kronecker product** of two endomorphisms $g_1 \in \operatorname{GL}(V_1)$ and $g_2 \in \operatorname{GL}(V_2)$ is the endomorphism $g_1\otimes g_2$ of $V_1\otimes_F V_2$ which acts as $(g_1\otimes g_2)(v_1\otimes v_2) = (g_1v_1)\otimes(g_2v_2)$ on decomposable elements, for all $v_1\in V_1$ and $v_2\in V_2$. If G and H are subgroups of $\operatorname{GL}_m(F)$, $\operatorname{GL}_n(F)$ respectively, we write $G\otimes H$ for the quotient of $G\times H$ by the equivalence relation

$$(a,b)\sim(c,d) \text{ if and only if there exists } \lambda\in F^\times \text{ such that } c=\lambda a,\ d=\lambda^{-1}b.$$

The group $G\otimes H$ is in a natural way a subgroup of $\operatorname{GL}_{mn}(F)$, the inclusion being given by identifying $(g,h)\in G\times H/\sim$ with $g\otimes h\in \operatorname{GL}_{mn}(F)$: the equivalence relation $\sim$ ensures that this identification is well defined ([BHRD13, Proposition 1.9.8]).

Finally, whenever G is a subgroup of a certain linear group $\operatorname{GL}_n(F)$, we write $\mathbb{P}G$ for the image of G in the quotient $\mathbb{P}\operatorname{GL}_n(F) := \dfrac{\operatorname{GL}_n(F)}{F^\times\cdot \operatorname{Id}}$. We break this convention only for the groups $\mathbb{P}\operatorname{SL}_n(F)$ and $\mathbb{P}\operatorname{GL}_n(F)$, which in homage to the tradition will be denoted simply by $\operatorname{PSL}_n(F)$ and $\operatorname{PGL}_n(F)$.

3.3 Maximal subgroups of $\operatorname{GSp}_{2n}(\mathbb{F}_\ell)$

We are now in a position to recall the classification of the maximal subgroups of $\operatorname{GSp}_{2n}(\mathbb{F}_\ell)$. For simplicity of exposition, and since this is the only case we will need, we assume from now on that ℓ is odd. Before stating the classification theorem we need to define some of the **Aschbacher classes**; we start with the notion of m-decomposition:

Definition 3.11. ([KL90, §4.2]) Let ℓ be an odd prime and $m\geq 2$ be an integer. An m-decomposition of $\mathbb{F}_\ell^{2n}$ is the data of m subspaces $V_1,\dots,V_m$ of $\mathbb{F}_\ell^{2n}$, each of dimension $\frac{2n}{m}$, such that

- the restriction of the standard symplectic form of $\mathbb{F}_\ell^{2n}$ to V_i is either nondegenerate for every $i=1,\dots,m$, or trivial for every $i=1,\dots,m$;
- $\mathbb{F}_\ell^{2n}\cong\bigoplus_{i=1}^m V_i$.

We can now define (some of) the Aschbacher classes; as the precise definition of class $\mathcal{C}_3$ is somewhat complicated (cf. [BHRD13, Definition 2.2.5]), we shall limit ourselves to giving the property that will be crucial to us.

Definition 3.12. A subgroup G of $\mathrm{GSp}_{2n}(\mathbb{F}_\ell)$ is said to be:

1. **reducible**, or of **class** $\mathcal{C}_1$, if it stabilizes a linear subspace of $\mathbb{F}_\ell^{2n}$;

2. **imprimitive**, or of **class** $\mathcal{C}_2$, if there exists an m-decomposition $V_1, \ldots, V_m$ which is stable under the action of G (i.e. for all $g \in G$ and for all $i = 1, \ldots, m$ there exists a $j \in \{1, \ldots, m\}$ such that $gV_i \subseteq V_j$);

3. **a field extension subgroup**, or of **class** $\mathcal{C}_3$, if there exist a prime s dividing $2n$, a structure of $\mathbb{F}_{\ell^s}$-vector space on $\mathbb{F}_\ell^{2n}$, and a subgroup H of G of index s such that H acts on $\mathbb{F}_\ell^{2n}$ preserving the $\mathbb{F}_{\ell^s}$-structure;

4. a **tensor product subgroup**, or of **class** $\mathcal{C}_4$, if there is a decomposition $\mathbb{F}_\ell^{2n} \cong V_1 \otimes V_2$ (where V_1, V_2 are $\mathbb{F}_\ell$-vector spaces) such that for each $g \in G$ there exist operators $g_1 \in \mathrm{GL}(V_1)$ and $g_2 \in \mathrm{GL}(V_2)$ that satisfy $g = g_1 \otimes g_2$.

5. a **tensor induced subgroup**, or of **class** $\mathcal{C}_7$, if there exist positive integers m, t (with $2n = (2m)^t$) and a decomposition $\mathbb{F}_\ell^{2n} \cong V_1 \otimes V_2 \otimes \cdots \otimes V_t$ (where $V_1, \ldots, V_t$ are $\mathbb{F}_\ell$-vector spaces all of the same dimension $2m$) with the following property: for all $g \in G$, there exist a permutation $\sigma \in S_t$ and operators $g_1, \ldots, g_t \in \mathrm{GSp}_{2m}(\mathbb{F}_\ell)$ such that $g(v_1 \otimes \cdots v_t) = (g_{\sigma(1)} v_{\sigma(1)}) \otimes \cdots (g_{\sigma(t)} v_{\sigma(t)})$ for all $v_1 \in V_1, \ldots, v_t \in V_t$. Such a G is isomorphic to the wreath product $\mathrm{GSp}_{2m}(\mathbb{F}_\ell) \wr S_t$.

We shall also have to deal with the exceptional class $\mathcal{S}$:

Definition 3.13. (cf. [BHRD13, Definition 2.1.3]) A subgroup G of $\mathrm{GSp}_{2n}(\mathbb{F}_\ell)$ is said to be of class $\mathcal{S}$ if and only if all of the following hold:

1. $\mathbb{P}G$ is almost simple;

2. G does not contain $\mathrm{Sp}_{2n}(\mathbb{F}_\ell)$;

3. G^∞ acts absolutely irreducibly on $\mathbb{F}_\ell^{2n}$.

It is a general philosophy (cf. for example [Ser86], especially §3, or [Die02, Remark 2.1]) that groups in class $\mathcal{S}$ should come in two different flavours. On one hand, there should exist finitely many groups $G_1, \ldots, G_k$ that embed in $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$ for infinite families of primes ℓ; we shall call them the **constant** (or **exceptional**) groups. On the other hand, there also exist maximal subgroups in class $\mathcal{S}$ **"of Lie type"**, obtained as follows. Given an algebraic group $\mathcal{G}$ over $\mathbb{Z}$ admitting an absolutely irreducible, symplectic representation of dimension $2n$, one can consider the corresponding map $\varphi : \mathcal{G} \to \mathrm{GSp}_{2n,\mathbb{Z}}$ and the subgroup $\varphi(\mathcal{G}(\mathbb{F}_\ell))$ of $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$: for ℓ sufficiently large, all the maximal subgroups in class $\mathcal{S}$ that are not "constant" should arise from this construction for suitable $\mathcal{G}$ and φ (and the groups $\mathcal{G}$ involved should be independent of ℓ – again, at least for ℓ large enough). We do not turn these notions into precise definitions, but it will be clear from sections 6 and 9 that there are indeed two different kinds of class-$\mathcal{S}$ subgroups, and that they need to be treated in different ways.

We are now finally ready to state the following classification theorem, essentially due to Aschbacher (but see also [BHRD13, Main Theorem and Table 3.5.C], [KL90], and [Lie85, §3]):

Theorem 3.14. *(Aschbacher [Asc84]) Let n be a positive integer and G be a maximal proper subgroup of $\mathrm{GSp}_{2n}(\mathbb{F}_\ell)$ not containing $\mathrm{Sp}_{2n}(\mathbb{F}_\ell)$. Then one of the following holds:*

1. *G is of class $\mathcal{C}_1$;*

2. *G is of class $\mathcal{C}_2$, stabilizing an m-decomposition for some $m \geq 2$ dividing $2n$;*

3. *G is of class $\mathcal{C}_3$ for some prime s dividing $2n$;*

4. *G is of class $\mathcal{C}_4$, and more precisely G is isomorphic to $\mathrm{GSp}_{2m}(\mathbb{F}_\ell) \otimes \mathrm{CGO}_t(\mathbb{F}_\ell)$, where m and $t \geq 3$ are integers such that $2mt = 2n$ (we call (m,t) the **type** of G);*

5. *G is of class $\mathcal{C}_7$ for some pair (m,t) such that $(2m)^t = 2n$;*

6. *G is of class $\mathcal{S}$;*

7. *we have $n = 2^m$, and $\mathbb{P}G$ contains as a subgroup of index at most 2 an extension of a group of order 2^{2m+1} by either $\mathrm{SO}^-_{2m}(2)$ or $\Omega^-_{2m}(2)$, according to whether ℓ is congruent to ± 1 or ± 3 modulo 8.*

Remark 3.15. Aschbacher's theorem is in fact a much more general statement, giving a classification of the maximal subgroups of all the finite classical groups, but in the present work we shall only need the case of $\mathrm{GSp}_{2n}(\mathbb{F}_\ell)$.

Remark 3.16. We shall not delve into the intricacies of orthogonal groups in even characteristic; all we need to know in order to prove theorem 1.2 is that the order of $\mathrm{SO}^-_{2m}(2)$ is given by ([BHRD13, Theorem 1.6.22])

$$2^{m^2-m}(2^m-1)\prod_{i=1}^{m-1}(2^{2i}-1),$$

and that $\Omega^-_{2m}(2)$ is a subgroup of $\mathrm{SO}^-_{2m}(2)$ (hence that the order of $\Omega^-_{2m}(2)$ does not exceed $2^{m^2-m-1}(2^m-1)\prod_{i=1}^{m-1}(2^{2i}-1)$). It is then immediate to show that in case (6) above we have

$$|\mathbb{P}G| < 2^{m^2+2m+2}\prod_{i=1}^{m-1}(2^{2i}-1) < (2n+3)!$$

so long as $m \geq 2$.

The proof of theorem 1.2 essentially consists in going through the list provided by theorem 3.14 to show that, for ℓ large enough, G_ℓ cannot be contained in any proper maximal subgroup of $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$, and therefore the equality $G_\ell = \mathrm{GSp}_{2g}(\mathbb{F}_\ell)$ must hold.

4 Reducible, imprimitive and field extension cases

Recall from the introduction that we denote by A/K an abelian variety of dimension g with $\mathrm{End}_{\overline{K}}(A) = \mathbb{Z}$, and by G_ℓ the image of the representation

$$\rho_\ell : \mathrm{Gal}\left(\overline{K}/K\right) \to \mathrm{Aut}\, A[\ell] \cong \mathrm{GL}_{2g}(\mathbb{F}_\ell).$$

At least for $\ell > b(A/K)$, we know from corollary 2.4 that (up to a choice of basis) we have $G_\ell \subseteq \mathrm{GSp}_{2g}(\mathbb{F}_\ell)$. Suppose now that G_ℓ does not contain $\mathrm{Sp}_{2g}(\mathbb{F}_\ell)$: then G_ℓ is contained in one of the maximal subgroups listed in theorem 3.14. The following proposition shows that cases 1 through 3 of that theorem cannot arise for ℓ large enough:

Proposition 4.1. *Let ℓ be a prime as in assumption 2.5. Let G be a maximal proper subgroup of $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$ that contains G_ℓ. Suppose G is*

1. *reducible: then $\ell \leq b_0(A/K)$.*
2. *imprimitive: then $\ell \leq b_0(A/K; g!)$.*
3. *a field extension subgroup: then $\ell \leq b_0(A^2/K; g)^{1/2g}$.*

Proof. Replacing K with an extension of degree at most $g!$ or g in cases 2 and 3, we can assume that G_ℓ stabilizes a subspace (cases 1 and 2), or that its centralizer in $\operatorname{End} A[\ell]$ is strictly larger than $\mathbb{F}_\ell$ (case 3). The claim then follows from [Lom14, Lemmas 3.17 and 3.18]. □

5 Groups of Lie type with socle $\mathrm{PSL}_2(\mathbb{F}_\ell)$

We now consider maximal class-$\mathcal{S}$ subgroups G of $\mathrm{GSp}_{2n}(\mathbb{F}_\ell)$ that satisfy $\mathrm{soc}(\mathbb{P}G) \cong \mathrm{PSL}_2(\mathbb{F}_\ell)$. There are various reasons why we single out this case. On one hand, it is not hard to construct (for all n and most ℓ) an explicit family of maximal subgroups of $\mathrm{GSp}_{2n}(\mathbb{F}_\ell)$ of this form, so this is clearly a case we need to treat. On the other hand, with the techniques of section 9 it is possible to show that, for most values of n, this is in fact the *only* kind of class-$\mathcal{S}$ subgroup of Lie type of $\mathrm{GSp}_{2n}(\mathbb{F}_\ell)$. Finally, considering this comparatively simple case on its own allows us to present some key ideas without the additional technical complications of §9.

To see how maximal subgroups of $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$ with projective socle $\mathrm{PSL}_2(\mathbb{F}_\ell)$ arise, denote by $V_1 := \mathbb{F}_\ell^2$ the defining representation of either $\mathrm{GL}_2(\mathbb{F}_\ell)$ or $\mathrm{SL}_2(\mathbb{F}_\ell)$, and consider, for every positive integer n, the $(2n-1)$-th symmetric power of V_1, which we denote by V_{2n-1}; it is a symplectic representation of $\mathrm{GL}_2(\mathbb{F}_\ell)$ or $\mathrm{SL}_2(\mathbb{F}_\ell)$ respectively. By [BHRD13, Proposition 5.3.6 (i)], for $\ell > 2n$ this representation is absolutely irreducible, and its image gives rise to a maximal class-$\mathcal{S}$ subgroup G of $\mathrm{GSp}_{2n}(\mathbb{F}_\ell)$ such that $\mathrm{soc}(\mathbb{P}G) \cong \mathrm{PSL}_2(\mathbb{F}_\ell)$. We denote by

$$\sigma_{2n-1} : \mathrm{GL}_2(\mathbb{F}_\ell) \to \mathrm{GSp}(V_{2n-1}) \cong \mathrm{GSp}_{2n}(\mathbb{F}_\ell)$$

the representation thus obtained, and by S_{2n-1} the image of $\mathrm{GL}_2(\mathbb{F}_\ell)$ in $\mathrm{GSp}_{2n}(\mathbb{F}_\ell)$. As the following lemma shows, the group S_{2n-1} is the only one we need to consider:

Lemma 5.1. *([BHRD13, Proposition 5.3.6 (i)]) Let $\ell > 2n$ be a prime number and let G be a maximal class-$\mathcal{S}$ subgroup of $\mathrm{GSp}_{2n}(\mathbb{F}_\ell)$ such that $\operatorname{soc} \mathbb{P}G \cong \mathrm{PSL}_2(\mathbb{F}_\ell)$. Then (up to conjugation in $\mathrm{GSp}_{2n}(\mathbb{F}_\ell)$) we have $\mathbb{P}G = \mathbb{P}S_{2n-1}$.*

We now turn to the application to abelian varieties. Suppose once more that A/K is an abelian variety of dimension g with $\mathrm{End}_{\overline{K}}(A) = \mathbb{Z}$, and suppose that for some prime $\ell > 2g$ the group G_ℓ is contained in a maximal class-$\mathcal{S}$ subgroup G of $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$ with projective socle $\mathrm{PSL}_2(\mathbb{F}_\ell)$. By the previous lemma, we can assume $\mathbb{P}G = \mathbb{P}S_{2g-1}$. In this situation, the assumption $G_\ell \subseteq G$ implies that for every $h \in G_\ell$ there exist a scalar $\lambda \in \mathbb{F}_\ell^\times$ and an element $M \in \mathrm{GL}_2(\mathbb{F}_\ell)$ such that $h = \lambda \cdot \sigma_{2g-1}(M)$. In particular, the eigenvalues of h are given by the (multi)set

$$\left\{ \lambda \mu^j \nu^{2g-1-j} \mid j = 0, \ldots, 2g-1 \right\}, \tag{2}$$

where μ, ν are the eigenvalues of M. Notice that the eigenvalues of M lie either in $\mathbb{F}_\ell$ or in its (unique) quadratic extension, hence all eigenvalues of h are elements of $\mathbb{F}_{\ell^2}$. We shall

now show that (for ℓ large enough) this description of the eigenvalues of h contradicts what is known about the representation ρ_ℓ restricted to the inertia at ℓ. More precisely, let $\mathfrak{l}$ be a place of K above the prime ℓ, let $I_\mathfrak{l} \subseteq \operatorname{Gal}\left(\overline{K}/K\right)$ be the inertia group at $\mathfrak{l}$, and write $I_\mathfrak{l}^t$ for the *tame* inertia group at $\mathfrak{l}$. Under a semistability hypothesis, the action of $I_\mathfrak{l}$ on $A[\ell]$ factors through $I_\mathfrak{l}^t$, and is described by the following theorem of Raynaud:

Theorem 5.2. *([Ray74, Corollaire 3.4.4]) Suppose A has semistable reduction at $\mathfrak{l}$: then the wild inertia subgroup of $I_\mathfrak{l}$ acts trivially on $A[\ell]$, so the action of $I_\mathfrak{l}$ factors through $I_\mathfrak{l}^t$. Let V be a Jordan-Hölder quotient of $A[\ell]$ for the action of $I_\mathfrak{l}^t$. Suppose V is of dimension n over $\mathbb{F}_\ell$, and let e be the ramification index of $\mathfrak{l}$ over ℓ. There exist integers $e_1, \ldots, e_n$ such that:*

- *V has a structure of $\mathbb{F}_{\ell^n}$-vector space;*
- *the action of $I_\mathfrak{l}^t$ on V is given by a character $\psi : I_\mathfrak{l}^t \to \mathbb{F}_{\ell^n}^\times$;*
- *$\psi = \varphi_1^{e_1} \ldots \varphi_n^{e_n}$, where $\varphi_1, \ldots, \varphi_n$ are the fundamental characters of $I_\mathfrak{l}^t$ of level n;*
- *for every $i = 1, \ldots, n$ the inequality $0 \leq e_i \leq e$ holds.*

Remark 5.3. Raynaud's theorem is usually stated for places of *good* reduction. However, as it was shown in [LV14, Lemma 4.9], the extension to the semistable case follows easily upon applying results of Grothendieck [Gro].

Remark 5.4. By construction the fundamental characters of level n are *surjective* morphisms $I_\mathfrak{l}^t \to \mathbb{F}_{\ell^n}^\times$. Moreover, the norm of a fundamental character of level n (taken from $\mathbb{F}_{\ell^n}$ to $\mathbb{F}_\ell$) is the unique fundamental character of level 1. When $\mathfrak{l}$ is unramified in K, this unique character of level 1 is χ_ℓ, the cyclotomic character mod ℓ.

Assumption. For the rest of this section we suppose that ℓ is a prime for which there exists a place $\mathfrak{l}$ of K of characteristic ℓ at which A has either good or bad semistable reduction. We suppose furthermore that ℓ is as in assumption 2.5, and that G_ℓ is contained in a maximal subgroup G of $\operatorname{GSp}_{2g}(\mathbb{F}_\ell)$ such that $\mathbb{P}G = \mathbb{P}S_{2g-1}$.

Let now $W_1, \ldots, W_k$ be the sequence of Jordan-Hölder quotients of $A[\ell]$ under the action of $I_\mathfrak{l}^t$, and $\psi_1, \ldots, \psi_k$ be the corresponding characters as in Raynaud's theorem. Also write $n_i = \dim W_i$ and suppose, for the rest of the section, that ℓ is unramified in K.

Lemma 5.5. *Let W be a simple Jordan-Hölder quotient of $A[\ell]$ of dimension n and let ψ be the associated character $I_\mathfrak{l}^t \to \mathbb{F}_{\ell^n}^\times$. The image of ψ is not contained in $\mathbb{F}_{\ell^k}^\times$ for any $k \mid n$, $k < n$.*

Proof. Suppose that the image of ψ is contained in $\mathbb{F}_{\ell^k}^\times$ for a certain $k \geq 1$, and let σ be a generator of $\operatorname{Gal}\left(\mathbb{F}_{\ell^k}/\mathbb{F}_\ell\right)$. Since the action of $I_\mathfrak{l}^t$ on W can be diagonalized over $\mathbb{F}_{\ell^k}$, we can find a vector $v \in W \otimes_{\mathbb{F}_\ell} \mathbb{F}_{\ell^k}$ that is a common eigenvector for the action of $I_\mathfrak{l}^t$. The $\mathbb{F}_{\ell^k}$-vector subspace of $W \otimes_{\mathbb{F}_\ell} \mathbb{F}_{\ell^k}$ spanned by $v, \sigma v, \ldots, \sigma^{k-1} v$ is by construction σ-stable, hence it descends to a $\mathbb{F}_\ell$-subspace W' of W, and it is clear by construction that W' is also stable under the action of $I_\mathfrak{l}^t$. As W is irreducible and W' is nontrivial we must have $W' = W$, and since $\dim W' \leq k$ we have $n = \dim W \leq k$ as claimed. □

Lemma 5.6. *We have $n_i \leq 2$ for all i.*

Proof. We have already remarked that all the eigenvalues of every element of G_ℓ lie in $\mathbb{F}_{\ell^2}$, hence in particular the same is true for the eigenvalues of the action of $I_{\mathfrak{l}}^t$. It follows that the image of ψ is entirely contained in $\mathbb{F}_{\ell^2}$, so the claim follows from the previous lemma. $\square$

In view of Raynaud's theorem and of the previous lemma, the only characters through which $I_{\mathfrak{l}}^t$ can act on $A[\ell]$ are the fundamental characters of level 1 and 2, along with the trivial character. Denote by m_0 (resp. m_1, m_2) the number of Jordan-Hölder quotients of $A[\ell]$ on which $I_{\mathfrak{l}}^t$ acts trivially (resp. through χ_ℓ, through one of the fundamental characters of level 2). As $A[\ell]$ is of dimension $2g$, the dimensions of its simple Jordan-Hölder quotients must add up to $2g$, and so we have

$$m_0 + m_1 + 2m_2 = 2g. \tag{3}$$

These three numbers also satisfy another numerical relation:

Lemma 5.7. *Suppose $\ell > g + 1$ is unramified in K: then $m_0 = m_1$.*

Proof. Notice that since ℓ is unramified in K the exponents e_i in Raynaud's theorem are all equal to either 0 or 1. Write $\varphi_1, \varphi_2 = \varphi_1^\ell$ for the two fundamental characters of level 2. If W is a simple Jordan-Hölder quotient of $A[\ell]$ of dimension 2, the action of $x \in I_{\mathfrak{l}}^t$ on W has eigenvalues $\varphi_1(x)$ and $\varphi_2(x)$, hence its determinant is $\varphi_1(x)\varphi_2(x) = \chi_\ell(x)$. On the other hand, the determinant of the action on 1-dimensional simple quotients is either 1 (if the action is trivial) or $\chi_\ell(x)$ (if the action is through χ_ℓ). It follows that

$$\chi_\ell(x)^g = \det\left(\rho_\ell(x) : A[\ell] \to A[\ell]\right) = \prod_{W_i} \det\left(\rho_\ell(x) : W_i \to W_i\right) = \chi_\ell(x)^{m_1} \chi_\ell(x)^{m_2} \quad \forall x \in I_{\mathfrak{l}}^t,$$

i.e. $\chi_\ell^{m_1+m_2-g} \equiv 1$ on $I_{\mathfrak{l}}^t$. Since ℓ is unramified in K, the order of the image of χ_ℓ is $\ell - 1$, hence we must have $(\ell - 1) \bigm| m_1 + m_2 - g$. However, $|m_1 + m_2 - g| \leq g$ by equation (3), and since $\ell - 1 > g$ by assumption the only possibility is $m_1 + m_2 = g$. Together with $m_0 + m_1 + 2m_2 = 2g$ this yields $m_0 = m_1$ as claimed. $\square$

The next step is to show that in fact there are no inertia invariants if ℓ is sufficiently large with respect to g:

Lemma 5.8. *Suppose $g \geq 3$. If $\ell > g(2g - 1) + 1$ is unramified in K, then $m_0 = 0$.*

Proof. The previous lemmas imply that $m_1 + m_2 = g \geq 3$, hence we have $\max\{m_1, m_2\} \geq 2$. Suppose by contradiction that $m_0 \geq 1$. By definition of m_0, m_1 and m_2, for every $x \in I_{\mathfrak{l}}^t$ the eigenvalues of $\rho_\ell(x)$ are $\left\{1, \chi_\ell(x), \varphi_1(x), \varphi_1(x)^\ell\right\}$, with multiplicities given respectively by m_0, m_1, m_2 and m_2. On the other hand, we know from (2) that the eigenvalues of $\rho_\ell(x)$ can be written as $\left\{\lambda \mu^j \nu^{2g-1-j} \bigm| j = 0, \ldots, 2g - 1\right\}$ for some $\lambda \in \mathbb{F}_\ell^\times$ and $\mu, \nu \in \mathbb{F}_{\ell^2}^\times$. Observe now that for all $x \in I_{\mathfrak{l}}^t$ the operator $\rho_\ell(x)$ admits an eigenvalue of multiplicity at least 2 (since $\max\{m_1, m_2\} \geq 2$) and it also has 1 among its eigenvalues (since $m_0 \geq 1$): thus there exist two indices $0 \leq j_1 < j_2 \leq 2g - 1$ (depending on x) such that $\lambda \mu^{j_1} \nu^{2g-1-j_1} = \lambda \mu^{j_2} \nu^{2g-1-j_2}$, and an index $0 \leq j_3 \leq 2g - 1$ (depending on x, and not necessarily distinct from j_1, j_2) such that $\lambda \mu^{j_3} \nu^{2g-1-j_3} = 1$. These equations can be rewritten as

$$\begin{cases} (\mu/\nu)^{j_1 - j_2} = 1 \\ \lambda = \mu^{-j_3} \nu^{j_3 - 2g + 1} = (\mu/\nu)^{-j_3} \nu^{1-2g}. \end{cases}$$

On the other hand, the fact that $\det \rho_\ell(x) = \chi_\ell(x)^g$ yields

$$\chi_\ell(x)^g = \det \rho_\ell(x) = \prod_{j=0}^{2g-1} \left(\lambda \mu^j \nu^{2n-1-j}\right) = \lambda^{2g} (\mu\nu)^{2g^2-g}, \tag{4}$$

and upon replacing λ by $(\mu/\nu)^{-j_3}\nu^{1-2g}$ we get $\chi_\ell(x)^g = (\mu/\nu)^{g(2g-1-2j_3)}$. Finally, raising both sides of this equation to the $(j_1 - j_2)$-th power and using $(\mu/\nu)^{j_1-j_2} = 1$ we find

$$\chi_\ell(x)^{g(j_1-j_2)} = (\mu/\nu)^{g(j_1-j_2)(2g-1-2j_3)} = 1,$$

which proves in particular that $\operatorname{ord} \chi_\ell(x) \leq g(j_2 - j_1) \leq g(2g-1)$ for all $x \in I_{\mathfrak{l}}^t$. Now since ℓ is unramified in K, the order of the (cyclic) group $\chi_\ell(I_{\mathfrak{l}}^t)$ is $\ell - 1 > g(2g-1)$: taking an $x \in I_{\mathfrak{l}}^t$ such that $\chi_\ell(x)$ generates $\chi_\ell(I_{\mathfrak{l}}^t)$ gives a contradiction, which shows that we must in fact have $m_0 = 0$. □

We have thus proved that for $\ell > g(2g-1)+1$ we necessarily have $m_0 = m_1 = 0$ and $m_2 = g$. It remains to show that this is impossible as well:

Lemma 5.9. *Suppose $\ell \geq 2g$ is unramified in K: then we cannot have $m_2 = g$.*

Proof. The proof is very similar to that of the previous lemma, so we keep the same notation. Let x be any element of $I_{\mathfrak{l}}^t$. Suppose by contradiction that we have $m_2 = g$. Then by an obvious pigeonhole argument we can find two indices $0 \leq j_1 < j_2 \leq 2g-1$ such that $j_2 - j_1 \leq 2$ and $\lambda\mu^{j_1}\nu^{2g-1-j_1} = \lambda\mu^{j_2}\nu^{2g-1-j_2}$, which implies $(\mu/\nu)^{j_2-j_1} = 1$ and therefore $\mu/\nu = \pm 1$. Moreover there exists an index $0 \leq j \leq 2g-1$ such that $\lambda\mu^j\nu^{2g-1-j} = \varphi_1(x)$, whence $\lambda^{2g} = \varphi_1(x)^{2g}\nu^{2g(1-2g)}$. Equation (4) now implies

$$\chi_\ell(x)^g = \lambda^{2g}(\mu\nu)^{g(2g-1)} = \varphi_1(x)^{2g}(\mu/\nu)^{g(2g-1)} = \pm\varphi_1(x)^{2g},$$

which, using $\chi_\ell(x) = \varphi_1(x)\varphi_2(x) = \varphi_1(x)^{\ell+1}$, implies $\varphi_1(x)^{g(\ell-1)} = \pm 1$ for all $x \in I_{\mathfrak{l}}^t$. This implies that the cyclic group $\varphi_1(I_{\mathfrak{l}}^t)$ has order at most $2g(\ell-1)$, but on the other hand we know that $\left|\varphi_1(I_{\mathfrak{l}}^t)\right| = \ell^2 - 1$: thus we obtain $\ell + 1 \leq 2g$, contrary to our assumptions, and we are done. □

Putting together the last three lemmas we have

Proposition 5.10. *Let ℓ be a prime as in assumption 2.5. Suppose $\ell > 2g(g-1)+1$ is unramified in K and such that there is at least one place $\mathfrak{l}$ of K of characteristic ℓ at which A has semistable reduction. Then G_ℓ cannot be contained in a maximal class-$\mathcal{S}$ subgroup G of $\operatorname{GSp}_{2g}(\mathbb{F}_\ell)$ with $\operatorname{soc} \mathbb{P}G \cong \operatorname{PSL}_2(\mathbb{F}_\ell)$.*

As promised in the introduction, we also give a version of this proposition in which we drop the semistability assumption, but we assume instead that we are given a place v as in the statement of theorem 1.2. The method of proof of this proposition will be generalized in section 9 to treat all class-$\mathcal{S}$ subgroups of Lie type.

Proposition 5.11. *Let ℓ be a prime as in assumption 2.5. Let v be a place of K, of good reduction for A, and such that the characteristic polynomial $f_v(x)$ of Fr_v has Galois group $(\mathbb{Z}/2\mathbb{Z})^g \rtimes S_g$. Suppose $\ell > (2q_v)^{[F(v):\mathbb{Q}]}$: then G_ℓ is not contained in a maximal class-$\mathcal{S}$ subgroup G of $\operatorname{GSp}_{2g}(\mathbb{F}_\ell)$ with $\operatorname{soc} \mathbb{P}G \cong \operatorname{PSL}_2(\mathbb{F}_\ell)$.*

Proof. Suppose by contradiction that G_ℓ is contained in a maximal class-$\mathcal{S}$ subgroup G of $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$ with $\operatorname{soc}\mathbb{P}G \cong \mathrm{PSL}_2(\mathbb{F}_\ell)$. Then, as we have seen, the eigenvalues of every operator $h \in G_\ell$ are of the form $\lambda\mu^i\nu^{2g-1-i}$ for some $\lambda,\mu,\nu \in \overline{\mathbb{F}_\ell}^\times$ and $i \in \{0,\dots,2g-1\}$; in particular, every such h possesses three eigenvalues

$$\overline{\mu_1} = \lambda\nu^{2g-1}, \quad \overline{\mu_2} = \lambda\mu\nu^{2g-2}, \quad \overline{\mu_3} = \lambda\mu^2\nu^{2g-3}$$

that satisfy $\overline{\mu_2}^2 = \overline{\mu_1}\cdot\overline{\mu_3}$. Now choosing $h = \rho_\ell(\mathrm{Fr}_v)$ – notice that clearly v does not divide ℓ, given the inequality $\ell > (2q_v)^{[F(v):\mathbb{Q}]}$ – we know that $\overline{\mu_1},\overline{\mu_2},\overline{\mu_3}$ are obtained by reduction in $\overline{\mathbb{F}_\ell}$ from three eigenvalues μ_1,μ_2,μ_3 of Fr_v. Furthermore, we have $\mu_2^2 \neq \mu_1\mu_3$ by lemma 2.12. By what we just showed, there is a place $\mathfrak{l}$ of $F(v)$, of characteristic ℓ, such that the nonzero algebraic integer $\mu_2^2 - \mu_1\mu_3$ has positive valuation at $\mathfrak{l}$: in particular, the norm $N_{F(v)/\mathbb{Q}}(\mu_2^2-\mu_1\mu_3)$ has positive valuation at $\mathfrak{l}$; but this is an integer, so it must be divisible by ℓ. On the other hand, as in the proof of lemma 2.14 it is easy to see that the Weil conjectures imply $|N_{F(v)/\mathbb{Q}}(\mu_2^2-\mu_1\mu_3)| \leq (2q_v)^{[F(v):\mathbb{Q}]}$. It follows that ℓ divides a nonzero integer that is at most $(2q_v)^{[F(v):\mathbb{Q}]}$, which clearly contradicts the inequality $\ell > (2q_v)^{[F(v):\mathbb{Q}]}$. ∎

6 Constant groups in class $\mathcal{S}$

The analysis of the constant subgroups of $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$ is greatly simplified by the following theorems of Larsen-Pink and Collins:

Theorem 6.1. *(Larsen-Pink [LP11, Theorem 0.2]) For every positive integer n there exists a constant $J'(n)$ with the following property: any finite subgroup Γ of $\mathrm{GL}_n(k)$ over any field k possesses normal subgroups $\Gamma_3 \subset \Gamma_2 \subset \Gamma_1$ such that*

- *(a)* $[\Gamma : \Gamma_1] \leq J'(n)$;
- *(b) either $\Gamma_1 = \Gamma_2$, or $p := \mathrm{char}(k)$ is positive and Γ_1/Γ_2 is a direct product of finite simple groups of Lie type in characteristic p;*
- *(c) Γ_2/Γ_3 is abelian, of order not divisible by $\mathrm{char}(k)$;*
- *(d) either $\Gamma_3 = \{1\}$, or $p := \mathrm{char}(k)$ is positive and Γ_3 is a p-group.*

Theorem 6.2. *([Col08, Theorem A]) One can take $J'(n) := \begin{cases} (n+2)!, & \text{if } n \geq 71 \\ n^4(n+2)!, & \text{if } n < 71 \end{cases}$, which is also optimal for $n \geq 71$. Furthermore, if in the previous theorem we restrict to fields k such that $\mathrm{char}\, k \nmid (n+1)(n+2)$, then one can replace $J'(n)$ by $J(n) := \begin{cases} (n+1)!, & \text{if } n \geq 71 \\ n^4(n+2)!, & \text{if } n < 71 \end{cases}$*

Remark 6.3. Collin's theorem is in fact more precise, and gives the optimal value of $J'(n)$ even in the case $n \leq 71$. Using this improved bound would not change our final result (theorem 1.2), and we have therefore chosen to state theorem 6.2 in the simple form given above.

Theorem 6.1 immediately implies:

Proposition 6.4. *Let ℓ, g be such that $\ell \nmid (2g+1)(2g+2)$. Suppose $G \subseteq \operatorname{GSp}_{2g}(\mathbb{F}_\ell)$ is a maximal subgroup of class $\mathcal{S}$ that satisfies $|\mathbb{P}G| > J(2g)$: then the socle of $\mathbb{P}G$ is a simple group of Lie type in characteristic ℓ.*

Proof. Apply theorem 6.1 to G. Notice first that Γ_3 is trivial: indeed, Γ_3 is a solvable normal subgroup of G, so $\mathbb{P}\Gamma_3$ is a solvable normal subgroup of $\mathbb{P}G$, which is almost-simple since G is of class $\mathcal{S}$. It follows from lemma 3.3 that $\mathbb{P}\Gamma_3$ is trivial, so Γ_3 is a subgroup of the group of homotheties in $\operatorname{GL}_{2g}(\mathbb{F}_\ell)$, which has order prime to ℓ. It follows that $\Gamma_3 = \{1\}$ as claimed. The same argument now shows that $\Gamma_2 \subseteq \mathbb{F}_\ell^\times \cdot \operatorname{Id}$, for otherwise $\mathbb{P}\Gamma_2$ would be an abelian (in particular solvable) normal subgroup of $\mathbb{P}G$. This implies in particular that Γ_1 and Γ_2 commute, and that $\mathbb{P}(\Gamma_1\Gamma_2) = \mathbb{P}\Gamma_1$. Notice that $\mathbb{P}\Gamma_1$ cannot be trivial, for otherwise we would have $|\mathbb{P}G| \leq J(2n)|\mathbb{P}(\Gamma_1)| = J(2n)$, contradicting the hypothesis; hence $\mathbb{P}\Gamma_1$ is a nontrivial normal subgroup of $\mathbb{P}G$, so it contains $\operatorname{soc}(\mathbb{P}G)$. On the other hand, the fact that Γ_2 consists entirely of homotheties implies that $\mathbb{P}\Gamma_1$ is a quotient of Γ_1/Γ_2, hence in particular a direct product of finite simple groups of Lie type in characteristic ℓ. Lemma 3.7 now implies that $\operatorname{soc}\mathbb{P}G = (\mathbb{P}\Gamma_1)^\infty$ is a finite simple group of Lie type in characteristic ℓ. □

The following proposition gives a linear lower bound on the order of $\mathbb{P}G_\ell$, which we will eventually use to show that the "constant" exceptional subgroups of $\operatorname{GSp}_{2g}(\mathbb{F}_\ell)$ can contain G_ℓ only for bounded values of ℓ:

Proposition 6.5. *Let ℓ be a prime such that there is a place $\mathfrak{l}$ of K of residual characteristic ℓ at which A has either good or bad semistable reduction. If ℓ is unramified in K and not less than $g+2$, then $|\mathbb{P}G_\ell| \geq \ell - 1$.*

Proof. We take the notation of section 5; in particular, we let $W_1, \ldots, W_k$ be the simple Jordan-Hölder quotients of $A[\ell]$ under the action of the inertia group $I_\mathfrak{l}$ (or equivalently, of the tame inertia group $I_\mathfrak{l}^t$), and $\psi_1, \ldots, \psi_k$ be the characters associated with the W_i (cf. theorem 5.2). Let N be the order of $|\mathbb{P}G_\ell|$, and notice that for every $y \in G_\ell$ the projective image of y^N is trivial, that is, y^N is a multiple of the identity, and in particular has a unique eigenvalue of multiplicity $2g$. Since for $x \in I_\mathfrak{l}^t$ the eigenvalues of $\rho_\ell(x)$ are given by the Galois conjugates of the various $\psi_i(x)$, this implies that for all $i, j = 1, \ldots, k$, for all integers $t \geq 0$, and for all $x \in I_\mathfrak{l}$ we have

$$\psi_i(x)^{\ell^t N} = \psi_j(x)^N. \tag{5}$$

We now distinguish three cases:

1. At least one of the W_i's is of dimension ≥ 2: without loss of generality, we can assume that $n := \dim W_1$ is at least 2. Let ψ be the associated character. By Raynaud's theorem, there are integers $e_0, \ldots, e_{n-1} \in \{0,1\}$ such that $\psi = \varphi^{\sum_{i=0}^{n-1} e_i \ell^i}$, where φ is a fundamental character of level n. Note that we cannot have $e_i = 1$ for $i = 0, \ldots, n-1$, for otherwise we would have $\psi = \chi_\ell$, which contradicts the fact that W_1 is of dimension $n > 1$ (lemma 5.5). In particular, since for all integers $t \geq 0$ the character φ^{ℓ^t} is a Galois conjugate of φ, replacing φ with φ^{ℓ^t} for a suitable t we can assume that $e_{n-1} = 0$ (notice that replacing φ with φ^ℓ has the effect of permuting cyclically the integers e_i, at least one of which is zero). Now φ has exact order $\ell^n - 1$, so $\psi = \varphi^{\sum_{i=0}^{n-1} e_i \ell^i}$ has order at least
$$\frac{\ell^n - 1}{\sum_{i=0}^{n-1} e_i \ell^i} \geq \frac{\ell^n - 1}{\sum_{i=0}^{n-2} \ell^i} = \frac{(\ell^n - 1)(\ell - 1)}{(\ell^{n-1} - 1)} \geq \ell(\ell - 1),$$

that is to say, there is an $x \in I_{\mathfrak{l}}^t$ such that $\psi(x)$ has order at least $\ell(\ell-1)$. Consider now equation (5) for this specific x, for $\psi_i = \psi_j = \psi$ and for $t = 1$: it gives $\psi(x)^{(\ell-1)\cdot N} = 1$, so $\psi(x)$ has order at most $(\ell-1)\cdot N$. Thus we obtain $(\ell-1)\cdot N \geq \ell(\ell-1)$, that is $N \geq \ell > \ell - 1$ as claimed.

2. All the W_i's are of dimension 1, for at least one index i we have $\psi_i = 1$, and for at least one index j we have $\psi_j = \chi_\ell$: then for all $x \in I_{\mathfrak{l}}^t$ we have $\psi_j(x)^N = \psi_i(x)^N$, that is, $\chi_\ell(x)^N = 1$ for all $x \in I_{\mathfrak{l}}^t$. As χ_ℓ has exact order $\ell - 1$, this implies $N \geq \ell - 1$.

3. All the W_i's are of dimension 1 and all characters ψ_i are equal to each other (and in particular are either all trivial or all equal to the cyclotomic character χ_ℓ): in this case there are exactly $k = 2g$ simple Jordan-Hölder quotients, and from the equality

$$\chi_\ell(x)^g = \det \rho_\ell(x) = \prod_{i=1}^{2g} \psi_i(x) = \begin{cases} 1, \text{ if } \psi_i = 1 \text{ for every } i \\ \chi_\ell(x)^{2g}, \text{ if } \psi_i = \chi_\ell \text{ for every } i \end{cases}$$

we find $\chi_\ell(x)^g = 1$ for all $x \in I_{\mathfrak{l}}^t$, which contradicts the fact that the order of χ_ℓ is $\ell - 1 > g$.

□

Corollary 6.6. *Let $\ell \geq J(2g)+2$ be a prime unramified in K. Suppose that there exists a place $\mathfrak{l}$ of K, of residual characteristic ℓ, at which A has semistable reduction: then $|\mathbb{P}G_\ell| > J(2g)$.*

Remark 6.7. Proposition 6.4 should be interpreted as saying that the order of the constant groups appearing as maximal subgroups of $\mathbb{P}\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$ is bounded by $J(2g)$ (for large enough g, equality is attained by the natural $2g$-dimensional representation of the symmetric group S_{2g+1}). Corollary 6.6 then amounts to saying that for $\ell > J(2g) + 1$ (and under a suitable semistability hypothesis) the action of Galois cannot factor through a constant group of class $\mathcal{S}$.

As promised, we also give a (much weaker) bound which however does not need any semistability assumption:

Proposition 6.8. *For every positive integer N we have $|\mathbb{P}G_\ell| > N$ so long as ℓ is strictly larger than $b_0(A/K;N)^{1/(2g-1)}$. Let ℓ be a prime as in assumption 2.5. If ℓ is larger than $b_0(A/K;J(2g))^{1/(2g-1)}$, and if G is a maximal subgroup of $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$ of class $\mathcal{S}$ such that $G_\ell \subseteq G$, then $\mathbb{P}G$ is an almost-simple group with socle of Lie type in characteristic ℓ.*

Proof. Let K' be the extension of K which is the fixed field of $\ker\left(\mathrm{Gal}\left(\overline{K}/K\right) \to \mathbb{P}G_\ell\right)$. By construction, the image of $\mathrm{Gal}\left(\overline{K'}/K'\right)$ in $\mathrm{Aut}\, A[\ell]$ consists entirely of scalars, so over K' the representation $A[\ell]$ admits an invariant subspace of dimension 1 (in fact, any subspace will do). Repeating the argument of [Lom14, Lemma 3.17] we find the desired result. The second part of the statement then follows from proposition 6.4, since under these hypotheses we have $|\mathbb{P}G| \geq |\mathbb{P}G_\ell| > J(2g)$. □

For future reference we record here the following fact (which follows from straightforward computations):

Lemma 6.9. *We have $b_0(A/K;J(2g))^{1/(2g-1)} < \max\{b(A/K;g!),\ b(A^2/K;g)^{1/2g}\}$.*

7 The tensor product case I – $\mathrm{GSp}_{2m}(\mathbb{F}_\ell) \otimes \mathrm{CGO}_n(\mathbb{F}_\ell)$, n odd

We now consider the problem of showing that, for ℓ large enough, the group G_ℓ cannot be contained in a tensor product subgroup of $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$. Let us briefly explain the key idea behind the proof, which goes back to Serre (cf. [Ser00a]). We shall be using the notation introduced in §2.3. If G_ℓ is contained in a tensor product subgroup, this forces the eigenvalues of any $x \in G_\ell$ to satisfy a number of additional multiplicative relations (besides the "obvious" ones that come from it being an element of $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$). On the other hand, the eigenvalues of most elements of $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$ do *not* satisfy these relations, so – in order to show that G_ℓ is not contained in a tensor product subgroup – it is enough to find a $g \in G_\ell$ whose eigenvalues do not satisfy any multiplicative relations except for the "obvious" ones. We shall look for such an element among those of the form $\rho_\ell(\mathrm{Fr}_v)$, where Fr_v is the Frobenius element attached to a place v of K: since the eigenvalues of $\rho_\ell(\mathrm{Fr}_v)$ are independent of ℓ, if for a certain prime ℓ_0 the eigenvalues of $\rho_{\ell_0}(\mathrm{Fr}_v)$ do not satisfy these additional relations, then the same is true for the eigenvalues of $\rho_\ell(\mathrm{Fr}_v)$ for all but finitely many primes ℓ. This will be enough to conclude that, for ℓ large enough, G_ℓ is not contained in a tensor product subgroup.

We split the analysis of tensor product subgroups into two parts: in this section and the next we show that, given such a "generic" Frobenius element, we can indeed give an explicit bound on the largest prime ℓ for which G_ℓ is contained in a tensor product subgroup; in section 12 we then show how, when $g = 3$, Chebotarev's density theorem enables us to find a suitable Frobenius element.

For the rest of this section we focus on the case of tensor products $\mathrm{GSp}_{2m} \otimes \mathrm{CGO}_n(\mathbb{F}_\ell)$ where n is odd, postponing the corresponding discussion for n even to section 8.

We shall need the following basic facts from group theory, whose proof is completely straightforward:

Lemma 7.1. *Let m, n be positive integers with n odd.*

1. *Let $\ell \geq 3$ be a prime. The groups $\mathrm{Sp}_{2m}(\mathbb{F}_\ell) \otimes \mathrm{SO}_n(\mathbb{F}_\ell)$ and $\mathrm{Sp}_{2m}(\mathbb{F}_\ell) \otimes \mathrm{GO}_n(\mathbb{F}_\ell)$ coincide.*
2. *Let F be a field not of characteristic 2 and h be an element of $\mathrm{SO}_n(F)$. The multiset Ψ of eigenvalues of h can be written as $\left\{\beta_1, \ldots, \beta_{\frac{n-1}{2}}, 1, \beta_1^{-1}, \ldots, \beta_{\frac{n-1}{2}}^{-1}\right\}$ for certain $\beta_1, \ldots, \beta_{\frac{n-1}{2}} \in \overline{F}^\times$.*
3. *Let $g = mn$ and G be a maximal subgroup of $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$ of tensor product type (m, n), that is, $G \cong \mathrm{GSp}_{2m}(\mathbb{F}_\ell) \otimes \mathrm{CGO}_n(\mathbb{F}_\ell)$. For every $h \in G$, the eigenvalues of h can be written as the multiset $\left\{\lambda_i\beta_j, \lambda_i, \lambda_i\beta_j^{-1} \mid i = 1, \ldots, 2m,\ j = 1, \ldots, \frac{n-1}{2}\right\}$ for certain $\lambda_1, \ldots, \lambda_{2m}, \beta_1, \ldots, \beta_{\frac{n-1}{2}}$ in $\overline{\mathbb{F}_\ell}^\times$.*

We now start investigating the multiplicative relations satisfied by the eigenvalues of an operator lying in a tensor product subgroup. Even though in general there may be additional relations, by part (3) of the previous lemma we already know a large number of equations these eigenvalues must satisfy; to state them more concisely, we introduce the following definition:

Definition 7.2. Let m, n be positive integers with n odd. We let V_{mn} be the affine scheme cut in $\mathbb{A}^{2g}_{\mathbb{Z}}$ (with variables $z_1, \ldots, z_{2m}$ and x_{ij}, y_{ij} for $i = 1, \ldots, 2m$ and $j = 1, \ldots, \frac{n-1}{2}$) by

the equations

$$\begin{cases} x_{ij}y_{ij} = z_i^2 & \text{for } i = 1, \dots, 2m \text{ and } j = 1, \dots, \frac{n-1}{2} \\ z_k x_{ij} = z_i x_{kj} & \text{for } i, k = 1, \dots, 2m \text{ and } j = 1, \dots, \frac{n-1}{2} \\ z_k y_{ij} = z_i y_{kj} & \text{for } i, k = 1, \dots, 2m \text{ and } j = 1, \dots, \frac{n-1}{2} \end{cases}$$

Remark 7.3. The variables x_{ij}, y_{ij}, z_i of this definition should be thought as corresponding respectively to the eigenvalues $\lambda_i\beta_j, \lambda_i\beta_j^{-1}$ and λ_i (notation as in lemma 7.1).

We denote by $\mathbf{v} = (z_k, x_{ij}, y_{ij})$ a point in $\mathbb{A}^{2g}_{\mathbb{Z}}$ and let elements $\sigma \in S_{2g}$ act on $\mathbb{A}^{2g}_{\mathbb{Z}}$ by permuting the coordinates in the natural way. For every $\sigma \in S_{2g}$ we consider the scheme V^σ_{mn} defined by $\left\{\mathbf{v} \in \mathbb{A}^{2g}_{\mathbb{Z}} \;\middle|\; \sigma(\mathbf{v}) \in V_{mn}\right\}$. We let $\mathcal{P}^\sigma_{mn}$ be a set of homogeneous binomials of degree 2 with coefficients in $\{\pm 1\}$ that generate the ideal defining V^σ_{mn}: it is clear by the definition of V that such polynomials exist. Finally, we let U^σ_{mn} be the complement of the closed subscheme of V^σ_{mn} defined by the vanishing of the function $\displaystyle\prod_{i=1}^m \left(z_i \prod_{j=1}^{(n-1)/2} x_{ij}y_{ij} \right)$, and to ease the notation we set $U_{mn} := U^{\mathrm{id}}_{mn}$.

Lemma 7.4. *Let F be a field. For a $2g$-tuple $(w_1, \dots, w_{2g})$ of elements of $F^\times$ the following are equivalent:*

1. *there exists a permutation $\sigma \in S_{2g}$ such that $(w_1, \dots, w_{2g}) \in U^\sigma_{mn}(F)$;*
2. *there exist $\lambda_1, \dots, \lambda_{2m}, \beta_1, \dots, \beta_{\frac{n-1}{2}} \in F^\times$ such that $w_1, \dots, w_{2g}$ equal (in some order) the $2g$ numbers $\lambda_i, \lambda_i\beta_j^{\pm 1}$ for $i = 1, \dots, 2m$ and $j = 1, \dots, \frac{n-1}{2}$.*

Proof. Notice that both conditions are invariant under the action of S_{2g}, so we consider the statement up to permutation of the coordinates. Assume first that (2) holds: then (up to permuting the w_i) we obtain a point of $U_{mn}(F)$ by setting, for $i = 1, \dots, 2m$ and $j = 1, \dots, \frac{n-1}{2}$,

$$\begin{cases} z_i = \lambda_i \\ x_{ij} = \lambda_i\beta_j \\ y_{ij} = \lambda_i\beta_j^{-1}. \end{cases}$$

Conversely, starting from a point $(w_1, \dots, w_{2g})$ in $U^\sigma_{mn}(F)$ as in (1), the invariance of the statement under permutations allows us to assume that $\sigma = \mathrm{id}$, and we get a decomposition as in (2) by setting $\lambda_i = z_i$ for $i = 1, \dots, 2m$ and $\beta_j = x_{1j}/z_1$ for $j = 1, \dots, \frac{n-1}{2}$. $\square$

Proposition 7.5. *Let v be a place of good reduction of A and m, n be positive integers such that $mn = g$ (with $n \geq 3$ odd). Let $(\mu_1, \dots, \mu_{2g})$ be the eigenvalues of Fr_v and suppose that*

$$(\mu_1, \dots, \mu_{2g}) \notin \bigcup_{\sigma \in S_{2g}} U^\sigma_{mn}(\overline{\mathbb{Q}}).$$

Let ℓ be a prime as in assumption 2.5. If ℓ is strictly larger than $(2q_v)^{[F(v):\mathbb{Q}]}$, then the element $\rho_\ell(\mathrm{Fr}_v)$ does not lie in a tensor product subgroup of $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$ of type (m, n). In particular, for any such ℓ the group G_ℓ is not contained in a tensor product subgroup of type (m, n).

Proof. Since clearly $\prod_{i=1}^{2g} \mu_i \neq 0$, the fact that $(\mu_1, \ldots, \mu_{2g})$ does not belong to $U^\sigma_{mn}\left(\overline{\mathbb{Q}}\right)$ for any σ is equivalent to the fact that for every $\sigma \in S_{2g}$ there is a $p^\sigma \in \mathcal{P}^\sigma_{mn}$ (cf. definition 7.2) such that $\alpha^\sigma_p := p^\sigma(\mu_1, \ldots, \mu_{2g})$ is nonzero; recall that p^σ is a homogeneous binomial of degree 2 with coefficients in $\{\pm 1\}$. Since the μ_i are algebraic integers, so are the α^σ_p; furthermore, every α^σ_p belongs to $F(v)$, the splitting field of $f_v(x)$. Finally, the Weil conjectures imply that the absolute value of every Galois conjugate of every μ_i is $q_v^{1/2}$, so we have $|\alpha^\sigma_p| \leq 2q_v$ under any embedding of $F(v)$ in $\mathbb{C}$: putting everything together we see that, for every fixed σ, the set of numbers $\left\{a^\sigma_p := N_{F(v)/\mathbb{Q}}\left(\alpha^\sigma_p\right) \bigm| p \in \mathcal{P}^\sigma_{mn}\right\}$ consists of integers of absolute value at most $(2q_v)^{[F(v):\mathbb{Q}]}$, not all equal to zero. Suppose now by contradiction that $\rho_\ell(\mathrm{Fr}_v)$ lies in a tensor product subgroup of type (m, n). By lemma 7.1, the eigenvalues $\overline{\mu_1}, \ldots, \overline{\mu_{2g}}$ of $\rho_\ell(\mathrm{Fr}_v)$ can be written as

$$\left\{\overline{\lambda_i},\ \overline{\lambda_i} \cdot \overline{\beta_j},\ \overline{\lambda_i} \cdot \overline{\beta_j}^{-1} \bigm| i = 1, \ldots, 2m,\ j = 1, \ldots, \frac{n-1}{2}\right\}$$

for some elements $\overline{\lambda_i}, \overline{\beta_j}$ of $\overline{\mathbb{F}_\ell}^\times$, and by lemma 7.4 there is a permutation σ such that $(\overline{\mu_1}, \ldots, \overline{\mu_{2g}})$ defines a point of $U^\sigma_{mn}(\overline{\mathbb{F}_\ell})$. This implies that (for this specific choice of σ) all the numbers a^σ_p reduce to 0 in $\overline{\mathbb{F}_\ell}$, and since the a^σ_p are integers this amounts to saying that ℓ divides all the a^σ_p (for $p \in \mathcal{P}^\sigma_{mn}$). However, we have seen that there is at least one polynomial $p \in \mathcal{P}^\sigma_{mn}$ for which a^σ_p is nonzero, so $\ell \bigm| a^\sigma_p$ implies $\ell \leq |a^\sigma_p| \leq (2q_v)^{[F(v):\mathbb{Q}]}$: this clearly contradicts our choice of ℓ, and the proposition is proved. $\square$

Serre has proved [Ser00a, p. 49] that if the Mumford-Tate group of A is $\mathrm{GSp}_{2g,\mathbb{Q}}$ and the Mumford-Tate conjecture is true for A, then places v as in the statement of the proposition do exist (in fact, a slight modification of his argument shows that they have density 1). Furthermore, as already remarked in the introduction (cf. theorem 1.4), these conditions are both true for all abelian varieties that satisfy $\mathrm{End}_{\overline{K}}(A) = \mathbb{Z}$ and whose dimension lies outside a certain explicit set of density zero.

Now notice that the condition of the previous proposition is essentially about the multiplicative independence of the eigenvalues of Fr_v. As we have already seen in §2.3, a sufficient condition that ensures multiplicative independence is that the Galois group of the characteristic polynomial $f_v(x)$ is as large as possible. The following lemma shows in particular that when $f_v(x)$ has maximal Galois group the corresponding Frobenius Fr_v satisfies the assumptions of proposition 7.5:

Lemma 7.6. *Let v be a place of K of good reduction for A such that the Galois group of $f_v(x)$ is the full Weyl group $\mathcal{W}_g := (\mathbb{Z}/2\mathbb{Z})^g \rtimes S_g$. Let $(\mu_1, \ldots, \mu_{2g})$ be the eigenvalues of Fr_v. Then for any choice of positive integers (m, n) with $n \geq 3$ odd and $mn = g$ the point $(\mu_1, \ldots, \mu_{2g})$ does not belong to $\bigcup_{\sigma \in S_{2g}} U^\sigma_{mn}(\overline{\mathbb{Q}})$.*

Proof. Notice first that $f_v(x)$ is irreducible, so the μ_i are in particular all distinct. Let λ, ν_1, ν_2 be any three distinct eigenvalues of Fr_v. By lemma 2.12 we cannot have $\lambda^2 = \nu_1\nu_2$: in particular, no permutation of the μ_i can define a point of $U_{mn}(\overline{\mathbb{Q}})$, because one of the equations defining U_{mn} is $z_1^2 = x_{11}y_{11}$. $\square$

8 The tensor product case II – $\mathrm{GSp}_{2m}(\mathbb{F}_\ell) \otimes \mathrm{CGO}_{2n}(\mathbb{F}_\ell)$

We now investigate the case of tensor products $\mathrm{GSp}_{2m}(\mathbb{F}_\ell) \otimes \mathrm{CGO}_{2n}(\mathbb{F}_\ell)$, where $2g = 4mn$. We shall only need a result analogue to lemma 7.6, so we fix from the start a place v of K, of good reduction for A, such that the characteristic polynomial $f_v(x)$ of the Frobenius at v has Galois group $(\mathbb{Z}/2\mathbb{Z})^g \rtimes S_g$.

Lemma 8.1. *Let n be a positive integer and h be an element of $\mathrm{CGO}^{\varepsilon}_{2n}(\mathbb{F}_\ell)$, where $\varepsilon \in \{+,-\}$. There exist $\lambda \in \overline{\mathbb{F}_\ell}^\times$, $k \in \{n-1, n\}$, and $\xi_1, \ldots, \xi_k \in \overline{\mathbb{F}_\ell}^\times$ such that the eigenvalues of h are given either by*

$$\lambda, -\lambda,\ \lambda\xi_1, \ldots, \lambda\xi_k, \lambda\xi_1^{-1}, \ldots, \lambda\xi_k^{-1},\ \text{if } k = n-1,$$

or by

$$\lambda\xi_1, \ldots, \lambda\xi_k, \lambda\xi_1^{-1}, \ldots, \lambda\xi_k^{-1},\ \text{if } k = n.$$

Proof. Let M be the matrix representing the bilinear form of which $\mathrm{CGO}^{\varepsilon}_{2n}(\mathbb{F}_\ell)$ is the group of similarities. By definition we have $h^t M h = \kappa \cdot M$ for some scalar $\kappa \in \mathbb{F}_\ell$ (the multiplier of h). Let ν be an eigenvalue of h with associated eigenvector $w \in \overline{\mathbb{F}_\ell}^{2n}$. Notice now that

$$h^t(Mw) = \kappa \cdot M h^{-1} w = \kappa \cdot M(\nu^{-1} w) = (\kappa/\nu) \cdot Mw,$$

so κ/ν is an eigenvalue of h^t, hence also of h. It follows easily that $\nu \mapsto \kappa/\nu$ is an involution of the (multi)set of eigenvalues of h. Since the only fixed points of $\nu \mapsto \kappa/\nu$ are $\pm\sqrt{\kappa}$ (where $\sqrt{\kappa}$ is a fixed square root of κ in $\overline{\mathbb{F}_\ell}^\times$), the multiset of eigenvalues of h can be written as

$$\underbrace{\{\sqrt{\kappa}, \ldots, \sqrt{\kappa}\}}_{r \text{ copies}} \sqcup \underbrace{\{-\sqrt{\kappa}, \ldots, -\sqrt{\kappa}\}}_{s \text{ copies}} \sqcup \coprod_{i=1}^{u} \{a_i, \kappa/a_i\},$$

where $\{a_1, \ldots, a_u\}$ is a certain (multi)set of representatives of the eigenvalues of h distinct from $\pm\sqrt{\kappa}$. Notice now that r, s have the same parity, because $r + s + 2u = 2n$. The claim then follows by taking $\lambda = \sqrt{\kappa}$, $\xi_i = a_i/\sqrt{\kappa}$ for $i = 1, \ldots, u$, $\xi_i = 1$ for $i = u+1, \ldots, u + \lfloor \frac{r}{2} \rfloor$, $\xi_i = -1$ for $i = u + \lfloor \frac{r}{2} \rfloor + 1, \ldots, u + \lfloor \frac{r}{2} \rfloor + \lfloor \frac{s}{2} \rfloor$, and $k = u + \lfloor \frac{r}{2} \rfloor + \lfloor \frac{s}{2} \rfloor$. ☐

Lemma 8.2. *Let v be a place of K of good reduction for A such that the Galois group of the characteristic polynomial $f_v(x)$ is $(\mathbb{Z}/2\mathbb{Z})^g \rtimes S_g$. Let ℓ be a prime as in assumption 2.5. Let $m \geq 1, n \geq 2$ be integers such that $4mn = 2g$, and suppose that $\ell > 2(2q_v)^{[F(v):\mathbb{Q}]}$: then G_ℓ is not contained in a tensor product group of type $\mathrm{GSp}_{2m}(\mathbb{F}_\ell) \otimes \mathrm{CGO}_{2n}(\mathbb{F}_\ell)$.*

Proof. Suppose by contradiction that G_ℓ is contained in a tensor product subgroup of type (m, n). Up to conjugation, for every element h of G_ℓ there exist operators $a \in \mathrm{GSp}_{2m}(\mathbb{F}_\ell)$ and $b \in \mathrm{CGO}_{2n}(\mathbb{F}_\ell)$ such that $h = a \otimes b$. Let $\nu_1, \ldots, \nu_{2m}$ be the eigenvalues of a and

$$\left\{\lambda, -\lambda, \lambda\xi_1, \ldots, \lambda\xi_k, \lambda\xi_1^{-1}, \ldots, \lambda\xi_k^{-1}\right\}$$

be the eigenvalues of b (where the pair $\lambda, -\lambda$ may or may not be necessary). Suppose first that $k \geq 2$: then $x_1 = \nu_1\lambda\xi_1$, $x_2 = \nu_1\lambda\xi_2$, $x_3 = \nu_2\lambda\xi_1^{-1}$, $x_4 = \nu_2\lambda\xi_2^{-1}$, $x_5 = \nu_2\lambda\xi_1$, $x_6 = \nu_2\lambda\xi_2$ are six eigenvalues of h that satisfy

$$\begin{cases} x_1x_3 = x_2x_4 \\ x_1x_6 = x_2x_5. \end{cases}$$

Let furthermore $x_7, \ldots, x_{2g}$ be the remaining eigenvalues of h, listed in any order. If we specialize this discussion to $h = \rho_\ell(\mathrm{Fr}_v)$, then $x_1, \ldots, x_{2g}$ can be recovered as the reduction in $\overline{\mathbb{F}_\ell}$ of the eigenvalues $\mu_1, \ldots, \mu_{2g}$ of Fr_v, these being elements of $F(v) \subset \overline{\mathbb{Q}}^\times$. As in proposition 7.5 it follows that (up to renumbering the μ_i) the integers $N_{F(v)/\mathbb{Q}}(\mu_1\mu_3 - \mu_2\mu_4)$ and $N_{F(v)/\mathbb{Q}}(\mu_1\mu_6 - \mu_2\mu_5)$ are divisible by ℓ, hence (in the notation of lemma 2.14) we have $\ell \mid f_1(\mu_1, \ldots, \mu_{2g})$. The inequalities of lemma 2.14 then imply $\ell \leq 2(2q_v)^{[F(v):\mathbb{Q}]}$, contradiction.

Suppose on the other hand that $k = 1$. Then necessarily $\pm\lambda$ are among the eigenvalues of b, so $x_1 = \nu_1\lambda\xi_1$, $x_2 = \nu_1\lambda$ and $x_3 = \nu_1\lambda\xi_1^{-1}$ are three eigenvalues of h that satisfy $x_2^2 = x_1x_3$, and (up to renumbering the μ_i) we have $\ell \mid f_2(\mu_1, \ldots, \mu_{2g})$. The second part of lemma 2.14 implies $\ell \leq (2q_v)^{[F(v):\mathbb{Q}]}$, again a contradiction. $\square$

9 Class-$\mathcal{S}$ subgroups of Lie type

In this section we study the maximal subgroups of $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$ of class $\mathcal{S}$ "of Lie type". More precisely, in view of the result of proposition 6.4, we are interested in the maximal class-$\mathcal{S}$ subgroups G of $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$ such that $\mathrm{soc}\,(\mathbb{P}G)$ is a simple group of Lie type in characteristic ℓ. From now on we assume $\ell \neq 2, 3$, so as to avoid the pathologies associated with the finite Suzuki and Ree groups.

9.1 Preliminaries on algebraic groups and root systems

Let G be a simple, simply connected algebraic group of rank r over an algebraically closed field. We fix a maximal torus T of G and write $\Lambda \cong \mathbb{Z}^r$ for its character group and $\{\alpha_1, \ldots, \alpha_r\}$ for its simple roots. The vector space $\Lambda \otimes \mathbb{R}$ is in a natural way an Euclidean space, and we write $(\cdot, \cdot)$ for its inner product.

If α is an element of Λ (in particular, if it is a root) we write $\alpha^\vee$ for $\frac{2\alpha}{(\alpha,\alpha)}$, and define the **fundamental weights** $\omega_1, \ldots, \omega_r$ as being the dual basis of $\alpha_i^\vee$ with respect to $(\cdot, \cdot)$. By definition, they satisfy $\left(\omega_i, \alpha_j^\vee\right) = \delta_{ij}$, and they are a $\mathbb{Z}$-basis of Λ (this comes from the fact that G is simply connected). It is also convenient to introduce the map $\langle \cdot, \cdot \rangle : \Lambda \times \Lambda \to \mathbb{Z}$ given by

$$\langle \lambda, \alpha \rangle := \left(\lambda, \alpha^\vee\right) = \frac{2(\lambda, \alpha)}{(\alpha, \alpha)},$$

which allows us to recast the duality between fundamental weights and simple roots in the compact form $\langle \omega_i, \alpha_j \rangle = \delta_{ij}$. Notice that we take the convention that $\langle \cdot, \cdot \rangle$ be linear in its first argument. A weight $\lambda \in \Lambda$ will be said to be **dominant** if $\langle \lambda, \alpha_i \rangle \geq 0$ for all $i = 1, \ldots, r$; equivalently, if it is an integral combination of the fundamental weights ω_i with non-negative coefficients. We denote by Λ^+ the cone of dominant weights. We can introduce a partial ordering (both on Λ and on Λ^+) by declaring that a weight λ is as least as large as a weight μ (in symbols, $\lambda \succeq \mu$) if and only if $\lambda - \mu$ can be written as a sum of simple roots with *non-negative* coefficients.

We also write Δ for the set of all roots of G, and Δ^+ for the subset of positive roots, i.e. those that can be written as integral linear combinations of the α_i with non-negative coefficients; we have $|\Delta| = 2|\Delta^+|$. We define the **Weyl vector** δ by the formula $\delta = \frac{1}{2}\sum_{\alpha \in \Delta^+} \alpha$, and recall ([Hum78, §13.3, Lemma A]) that $\delta = \sum_{i=1}^r \omega_i$.

The **Coxeter number** of G is defined to be the ratio $h := \frac{|\Delta|}{r} = \frac{2|\Delta^+|}{r}$. By the classification of simple root systems it is known that h does not exceed $4r$ (and in fact it is at most $2r$ so long as $r \geq 9$).

The **Cartan matrix** of a root system (relative to a given choice of simple roots) is the $r \times r$ matrix whose (i,j)-th entry is given by $C_{ij} = \langle \alpha_i, \alpha_j \rangle$. Writing a simple root α_i as a combination of the fundamental weights, $\alpha_i = \sum_{j=1}^{r} b_{ij}\omega_j$, and applying the linear map $\langle \cdot, \alpha_k \rangle$ to both sides of this equation we obtain $C_{ik} = b_{ik}$, so the Cartan matrix is the base-change matrix expressing the simple roots in terms of the fundamental weights. Moreover, C has the following property, which can be gleaned by direct inspection of tables I through IX of Bourbaki [Bou02]:

Lemma 9.1. *The matrix $C - 2\,\mathrm{Id}$ has non-positive entries and its diagonal coefficients vanish.*

Finally, recall that the **Weyl group** of G, denoted by $W(G)$, is the subgroup of $\mathrm{GL}(\Lambda \otimes \mathbb{R})$ generated by the reflections along the simple roots α_i, and that the same definition can also be used to introduce a notion of Weyl group for not necessarily irreducible root systems and for not necessarily connected Dynkin diagrams. If Δ (resp. D) is a root system (resp. the associated Dynkin diagram) we write $W(\Delta) = W(D)$ for the corresponding Weyl group.

We conclude this section of preliminaries with a simple lemma which is certainly well-known to experts, but for which we could not find any reference in the literature:

Lemma 9.2. *Suppose G is of rank r and let $\lambda \in \Lambda$ be a nonzero weight. The orbit of λ under the Weyl group of G contains at least $r+1$ distinct weights.*

Proof. Let D be the Dynkin diagram associated with the root system of G. By the orbit-stabilizer lemma it is enough to show that the stabilizer of λ has index at least $r+1$ in $W(D)$. Since every weight is $W(D)$-conjugated to a dominant weight, there is no loss of generality in assuming that λ is dominant. In this case, the stabilizer of λ is known to be generated by those reflections s_α along simple roots such that $s_\alpha \lambda = \lambda$ ([Hum78, §10.3B]). Since the stabilizer of λ is clearly not the full Weyl group $W(D)$, there is at least one simple root β whose associated reflection does not stabilize λ. The stabilizer of λ is then identified to a subgroup of the group generated by s_α for all simple roots $\alpha \neq \beta$; notice that the group generated by $\left\{ s_\alpha \;\middle|\; \alpha \text{ a simple root}, \alpha \neq \beta \right\}$ is isomorphic to the Weyl group of the Dynkin diagram obtained from D by erasing the node corresponding to β. We thus obtain the following procedure for determining a lower bound for the index of $\mathrm{Stab}(\lambda)$ in $W(D)$: we consider the Dynkin diagram D and all the (quite possibly non-connected) diagrams $D_1, \ldots, D_r$ which we can obtain from D by erasing exactly one node. We then compute the Weyl groups $W(D_i)$ associated with each of these diagrams and the indices $|W(D)/W(D_i)|$: the smallest such index is a lower bound for the index $|W(D)/\mathrm{Stab}(\lambda)|$. The lemma now follows from a straightforward, if somewhat tedious, examination of the connected Dynkin diagrams and of table 1. As an example, let us do this for root systems of type A_r, which give the smallest possible index. Removing the i-th node ($i = 1, \ldots, r$) from the Dynkin diagram for A_r leads to the Dynkin diagram for the root system $A_{i-1} \times A_{r-i}$, where by $A_0 \times A_{r-1}$ and $A_{r-1} \times A_0$ we simply mean A_{r-1}. The Weyl group of this root system is $S_i \times S_{r-i+1}$, whose index in the Weyl group of A_r is $\frac{(r+1)!}{(i)!(r-i+1)!} = \binom{r+1}{i} \geq r+1$. ∎

Root system	Order of the Weyl group
A_r	$(r+1)!$
B_r	$2^r r!$
C_r	$2^r r!$
D_r	$2^{r-1} r!$
E_6	$72 \cdot 6!$
E_7	$72 \cdot 8!$
E_8	$192 \cdot 10!$
F_4	1152
G_2	12

Table 1: Orders of the Weyl groups (simple root systems)

9.2 Representation theory of finite simple groups of Lie type

This paragraph is essentially taken from [Lüb01], which will be our main reference for this section; further information can be found in [Car85], Chapter 1 (especially sections 1.17-1.19). Let $\tilde{G}$ be a finite twisted or non-twisted simple Chevalley group in characteristic $\ell \neq 2, 3$ (that is, a finite simple group of Lie type of characteristic different from 2 and 3; in particular, not a Suzuki or a Ree group). We shall describe shortly the main algebraic data associated with $\tilde{G}$, but before doing so we need to define Frobenius maps:

Definition 9.3. Let k be an algebraically closed field of characteristic $\ell > 0$, and let $q = \ell^e$ (where e is a positive integer). The q-Frobenius map of $\mathrm{GL}_n(k)$, denoted F_q, is the automorphism of $\mathrm{GL}_n(k)$ that raises all coefficients of a matrix to the q-th power. Let G be a linear algebraic group over k. A **standard Frobenius map** is a group morphism $F : G(k) \to G(k)$ such that, for some embedding $i : G(k) \hookrightarrow \mathrm{GL}_n(k)$ and for some $q = \ell^e$, the identity $i(F(g)) = F_q(i(g))$ holds for every $g \in G(k)$. Finally, a group morphism $G(k) \to G(k)$ is a **Frobenius map** (or endomorphism) if some power of it is a standard Frobenius map.

It is known that to a group $\tilde{G}$ as above we can attach a connected reductive simple algebraic group G over $\overline{\mathbb{F}_\ell}$ of simply connected type and a Frobenius endomorphism F of G with the following property: denoting by G^F the group $\left\{g \in G(\overline{\mathbb{F}_\ell}) \;\middle|\; F(g) = g\right\}$ of fixed points of F, and by Z the center of G^F, we have $\tilde{G} \cong G^F/Z$. Furthermore, G^F is the universal covering group (also known as the universal perfect central extension) of $\tilde{G}$, see [Gri73] and the references therein.

Remark 9.4. It is further known that the Frobenius endomorphism F is completely characterised by the choice of an automorphism of the Dynkin diagram of G together with a real number q which, in our setting (characteristic at least 5), is an integral power of ℓ (see for example [Hum06, §1.3]). We include this number q among the data associated with $\tilde{G}$; it will appear for example in the statement of theorem 9.5 and in the proof of lemma 9.25.

In this situation, we shall call G the algebraic group associated with $\tilde{G}$, and we shall indifferently speak of the rank of $\tilde{G}$, of G^F, or of G; likewise, we shall say that $\tilde{G}, G^F$, or G, is of type A_r (resp. $B_r, C_r, \ldots$) if the root system of G is.

Our interest in this construction comes from the fact that projective representations of $\tilde{G}$ in characteristic ℓ are the same as linear representations of G^F in characteristic ℓ ([Ste68,

pp. 76-77, items (ix) and (x)]), which in turn can be constructed by restricting algebraic representations of the algebraic group G to G^F, as we now describe. Let G be of rank r, denote by Λ^+ the cone of its dominant weights (with respect to a given maximal torus), and write $\omega_1, \ldots, \omega_r$ for the fundamental ones; for any given dominant weight $\lambda \in \Lambda^+$, the irreducible $\overline{\mathbb{F}_\ell}[G]$-module with highest weight λ will be denoted by $L(\lambda)$. The relationship between representations of G^F and algebraic representations of G is nicely described by the following theorem of Steinberg:

Theorem 9.5. *(Steinberg [Ste63]) Let G, G^F and q be as above (with the restriction that the characteristic be different from $2, 3$). Define*

$$\Lambda_q = \left\{ a_1\omega_1 + \cdots + a_r\omega_r \;\middle|\; 0 \leq a_i \leq q-1 \text{ for } 1 \leq i \leq r \right\}.$$

The restrictions of the G-modules $L(\lambda)$ with $\lambda \in \Lambda_q$ to G^F form a set of pairwise inequivalent representatives of all equivalence classes of irreducible $\overline{\mathbb{F}_\ell}[G^F]$-modules.

9.3 Some structure theorems

In this section we recall further results that describe more finely the structure of the simple modules $L(\lambda)$. It is useful to introduce the notion of (m-)restricted weights:

Definition 9.6. Let G, G^F be as above and m be a positive integer. A dominant weight $\lambda = a_1\omega_1 + \cdots + a_r\omega_r \in \Lambda^+$ is said to be m-restricted if for every $i = 1, \ldots, r$ we have $0 \leq a_i \leq m-1$.

Definition 9.7. Let F be an automorphism of a group $\tilde{G}$ and $\rho : \tilde{G} \to \mathrm{Aut}(V)$ be a representation of $\tilde{G}$. The **twist** of ρ by F is the representation ${}^F\rho$ given by ${}^F\rho(g) = \rho(F(g))$ for all $g \in G$. Note that twisting the representation does not change its image, nor its dimension.

The field automorphism $x \mapsto x^\ell$ of $\overline{\mathbb{F}_\ell}$ can be used to construct a canonical endomorphism of the algebraic group G, called the 'standard Frobenius map' and denoted by F_0 ([Hum06, §2.7]). The following theorem elucidates the importance of ℓ-restricted weights and their interactions with Frobenius twists:

Theorem 9.8. *(Steinberg's twisted tensor product theorem [Ste63]) If L is a G-module, let $L^{(i)}$ be the module obtained by twisting the G-action on L by F_0^i. If $\lambda_0, \ldots, \lambda_m$ are ℓ-restricted weights, then*

$$L(\lambda_0 + \ell\lambda_1 + \cdots + \ell^m\lambda_m) \cong L(\lambda_0) \otimes L(\lambda_1)^{(1)} \otimes \cdots \otimes L(\lambda_m)^{(m)}.$$

Theorems 9.5 and 9.8 are all we need to describe representations over $\overline{\mathbb{F}_\ell}$. However, to deal with groups with socle $\mathrm{PSL}_2(q)$, where q is a power of ℓ different from ℓ, it is not enough to work over $\overline{\mathbb{F}_\ell}$, but we shall need to know in which circumstances an $\overline{\mathbb{F}_\ell}$-representation can be defined over $\mathbb{F}_\ell$. We make this notion more precise in the following definition:

Definition 9.9. Let $\tilde{G}$ be a finite group, K a field, and $\rho : \tilde{G} \to \mathrm{GL}_n(K)$ a representation of $\tilde{G}$ over K. We say that ρ can be defined over a field $k \subseteq K$ if there exists a representation $\rho_k : \tilde{G} \to \mathrm{GL}_n(k)$ such that the representation

$$\tilde{G} \xrightarrow{\rho_k} \mathrm{GL}_n(k) \hookrightarrow \mathrm{GL}_n(K)$$

is isomorphic to ρ over K.

The fields of definition of modular representations of finite groups of Lie type are very well understood (cf. [BHRD13, Theorem 5.1.13]). Here we just need the simplest case, namely a criterion to decide whether a representation can be defined over $\mathbb{F}_\ell$.

Let $\ell \neq 2,3$. Write the number q associated with G^F (cf. remark 9.4) as ℓ^e. Let M be an irreducible $\overline{\mathbb{F}_\ell}[G^F]$-module. By theorem 9.5, M can be obtained as the restriction to G^F of an irreducible G-module which we still denote by M. As a representation of G, we have $M \cong L(\lambda)$, where (again by theorem 9.5) λ is ℓ^e-restricted. In particular, λ can be written as $\lambda_0 + \ell\lambda_1 + \cdots + \ell^{e-1}\lambda_{e-1}$, where the weights $\lambda_0, \ldots, \lambda_{e-1}$ are ℓ-restricted. Using theorem 9.8 we can then write M as a tensor product $\bigotimes_{i=0}^{e-1} M_i^{(i)}$, where M_i corresponds to λ_i.

Proposition 9.10. *With the above notation, the G^F-module M can be defined over $\mathbb{F}_\ell$ if and only if $M_i \cong M_j$ for all i,j.*

Proof. This follows at once from the proof of [BHRD13, Theorem 5.1.13]. More specifically, by [BHRD13, Corollary 1.8.14] M can be defined over $\mathbb{F}_\ell$ if and only if it is stabilized by the Frobenius automorphism F_0. On the other hand, we see from [BHRD13, Proposition 5.1.9 (v)] that twisting by F_0^e sends M_0 to an irreducible module defined by an ℓ-restricted weight, so M is isomorphic to $M^{(1)}$ if and only if $\bigotimes_{i=0}^{e-1} M_i^{(i)} \cong \bigotimes_{i=0}^{e-1} M_{i-1}^{(i)}$, where $M_{-1} = M_{e-1}^{(e)}$. Since the representation of theorem 9.8 is unique, this implies $M_{i-1} \cong M_i$ for $i = 1, \ldots, e-1$. $\square$

9.4 Duality

We shall also need some information about the duality properties of our representations; recall that the Frobenius-Schur indicator of an irreducible representation is $+1$ if that representation is orthogonal, -1 if it is symplectic, and 0 if it is not self-dual. Regarding the Frobenius-Schur indicator of the modular representations we are interested in we have the following result of Steinberg ([Ste68, Lemmas 78 and 79], but cf. also [Lüb01, §6.3]):

Theorem 9.11. *Assume $\ell \neq 2,3$. Write Z for the center of $G(\overline{\mathbb{F}_\ell})$ and let $\lambda = \sum_{i=1}^r a_i\omega_i$ be a q-restricted, dominant weight. Then*

- *if G is of type A_r, or D_r with odd r, or E_6, then the representations $L\left(\sum_{i=1}^r a_i\omega_i\right)$ and $L\left(\sum_{i=1}^r a_{\tau(i)}\omega_i\right)$, where the permutation τ is given by the automorphism of order two of the Dynkin diagram, are dual to each other. For any other G all representations $L(\lambda)$ are self-dual;*
- *there is an element $h \in Z$, of order at most 2, such that every self-dual module $L(\lambda)$ is symplectic if and only if h acts nontrivially on $L(\lambda)$.*

It is then relatively easy to work out which representations $L(\lambda)$ are symplectic; notice however that theorem 9.11 is quoted incorrectly in [Lüb01], and as a consequence the algorithm described in that paper to decide whether $L(\lambda)$ is symplectic or orthogonal does not yield correct results (for example, it implies the existence of symplectic representations of $\mathrm{Spin}(7, \mathbb{F}_p)$ for all sufficiently large primes p, which is not the case). The following result follows from theorem 9.11 (see also the proof of [TZ14, Proposition 5.3]); the numbering of the simple roots we use is that of [Bou02].

Corollary 9.12. *Assume $\ell \neq 2,3$. In the situation of the previous theorem, the representation $L(\lambda)$ of the finite group of Lie type G^F is symplectic if and only if:*

- *G is of type A_r, $r \equiv 1 \pmod 4$, $a_i = a_{r+1-i}$ for $i = 1, \dots, r$, and $a_{(r+1)/2}$ is odd, or*
- *G is of type B_r, $r \equiv 1, 2 \pmod 4$, and a_r is odd, or*
- *G is of type C_r, and $a_1 + a_3 + \dots + a_{2\lceil r/2 \rceil - 1}$ is odd, or*
- *G is of type D_r, $r \equiv 2 \pmod 4$, $a_{r-1} + a_r$ is odd, or*
- *G is of type E_7, and $a_2 + a_4 + a_7$ is odd.*

Corollary 9.13. *Let $q = \ell^e$ be the invariant attached to G^F, and let M be an absolutely irreducible, symplectic $\mathbb{F}_\ell[G^F]$-module. Then one of the following holds:*

1. *$e = 1$, that is, $q = \ell$, and we have $M \cong L(\lambda)$ for a certain ℓ-restricted weight that satisfies the conditions of corollary 9.12;*
2. *e is odd and greater than 1, and $\dim_{\mathbb{F}_\ell} M$ is a perfect e-th power. Furthermore, the Lie type of G is listed in the previous corollary, and $M \otimes_{\mathbb{F}_\ell} \overline{\mathbb{F}_\ell}$ is a tensor-decomposable G^F-module.*

Proof. Let $\overline{M} := M \otimes \overline{\mathbb{F}_\ell}$ and λ be the associated dominant q-restricted weight. We can write $\lambda = \sum_{i=0}^{e-1} \ell^i \lambda_i$, where each λ_i is ℓ-restricted. By theorem 9.8 we have $\overline{M} \cong \bigotimes_{i=0}^{e-1} L(\lambda_i)^{(i)}$, and since by assumption $\overline{M}$ can be defined over $\mathbb{F}_\ell$ proposition 9.10 gives $L(\lambda_i) \cong L(\lambda_j)$ for all i, j. It follows that $\dim(L_\lambda) = (\dim L(\lambda_0))^e$. Now if $e = 1$ we are in case (1) and we are done (by definition we have $q = \ell^e = \ell$). If instead we have $e > 1$ (in which case $\overline{M}$ is clearly tensor-decomposable) then we need to show that e is odd. Suppose on the contrary that e is even. By the discussion following [BHRD13, Proposition 5.1.12] we know that $L(\lambda_0)$ is self-dual. Now by theorem 9.11 there is an element h in the center of G^F that acts nontrivially on $L(\lambda_0)$ if and only if the latter is symplectic. Since h is central and $L(\lambda_0)$ is absolutely irreducible, h is a scalar; furthermore, since the order of h is at most 2, we must necessarily have $h = \pm 1$. It follows that h acts on $\overline{M} \cong \otimes_{i=0}^{e-1} L(\lambda_0)^{(i)}$ as $(\pm 1)^e$, so $\overline{M}$ is symplectic if and only if $h = -1$ and e is odd. Finally, G^F admits a symplectic representation, so its Lie type is listed in the previous corollary. This concludes the proof. ∎

9.5 Weyl modules

We briefly recall the basic properties of the so-called Weyl modules; for more information, cf. [Hum06, §3.1]. For any $\lambda \in \Lambda^+$ there is a certain $\mathbb{Z}G$-module $V(\lambda)_\mathbb{Z}$ such that

- the module $L(\lambda)$ is a quotient of $V(\lambda)_\mathbb{Z} \otimes_\mathbb{Z} \overline{\mathbb{F}_\ell}$;
- for a complex, simply connected, simple Lie group $G_\mathbb{C}$ with the same root system as G, the $\mathbb{C}G$-module $V(\lambda)_\mathbb{C} := V(\lambda)_\mathbb{Z} \otimes_\mathbb{Z} \mathbb{C}$ is the unique irreducible module of highest weight λ.

Definition 9.14. We call $V(\lambda)_\mathbb{Z} \otimes_\mathbb{Z} \overline{\mathbb{F}_\ell}$ the **Weyl module** associated with λ. It is a $\overline{\mathbb{F}_\ell}[G]$-module which we will denote simply by $V(\lambda)$.

A celebrated formula due to Weyl gives the dimension of $V(\lambda)$:

Theorem 9.15. *(Weyl) For all dominant weights λ we have*

$$\dim_{\overline{\mathbb{F}_\ell}} V(\lambda) = \dim_\mathbb{C} V(\lambda)_\mathbb{C} = \frac{\prod_{\alpha \in \Delta^+} (\lambda + \delta, \alpha)}{\prod_{\alpha \in \Delta^+} (\lambda, \alpha)},$$

where $\delta = \frac{1}{2} \sum_{\alpha \in \Delta^+} \alpha = \sum_{i=1}^r \omega_i$.

9.5.1 A sufficient condition for the equality $V(\lambda) = L(\lambda)$

In general, it can very well happen that $\dim_{\overline{\mathbb{F}_\ell}} L(\lambda)$ is strictly smaller than $\dim_{\overline{\mathbb{F}_\ell}} V(\lambda)$. The following theorem gives interesting information about the action of G^F on Weyl modules, which we shall use to deduce a sufficient condition for $V(\lambda)$ and $L(\lambda)$ to be isomorphic.

Theorem 9.16. *(Wong, [Won72, (2D)], [Hum06, §5.9]) If λ is a q-restricted, dominant weight, the Weyl module $V(\lambda)$ is indecomposable (but not necessarily irreducible) upon restriction to G^F. In particular, it is also indecomposable under the action of G.*

Since $V(\lambda)$ has highest weight λ by construction, $V(\lambda)$ admits a unique G-simple quotient that is the unique irreducible representation of G with highest weight λ; that is to say, $L(\lambda)$ is the unique simple quotient of $V(\lambda)$. We shall now see that, under suitable assumptions on the dimension of $V(\lambda)$ and on ℓ, we must in fact have $V(\lambda) = L(\lambda)$. The key result we need is the following theorem of McNinch (which builds on previous work of Jantzen, [Jan97]).

Theorem 9.17. *([McN98]) Let k be an algebraically closed field of characteristic $\ell \geq 7$, and suppose that the root system of G is not of type A_1. Let furthermore V be a module over $k[G^F]$ such that $\dim_k V \leq 2\ell$: then V is semisimple.*

Corollary 9.18. *Suppose G is not of Lie type A_1. If λ is a dominant and q-restricted weight, ℓ is at least 7, and $\dim V(\lambda) \leq 2\ell$, then $L(\lambda) \cong V(\lambda)$.*

Proof. Notice that an indecomposable and semisimple module is simple. Hence in particular $V(\lambda)$ is G^F-simple by the combination of the previous theorems, and since $L(\lambda)$ is the unique simple (nonzero) quotient of $V(\lambda)$ the two must coincide. □

9.5.2 The case $V(\lambda) \neq L(\lambda)$

When $L(\lambda)$ does not coincide with $V(\lambda)$ its precise structure is still quite mysterious and forms the subject of a rich body of work. For our applications, however, we shall just need to know that the dimension of $L(\lambda)$ grows reasonably quickly when the coefficients a_i in the representation $\lambda = \sum a_i\omega_i$ go to infinity. To prove such an estimate we shall need the following theorem of Premet:

Theorem 9.19. *([Pre87]) Let G be a simple, simply connected algebraic group in characteristic ℓ. If the root system of G has different root lengths we assume that $\ell \neq 2$, and if G is of type G_2 we also assume that $\ell \neq 3$. Let λ be an ℓ-restricted dominant weight. The set of weights of the irreducible G-module $L(\lambda)$ is the union of the $W(G)$-orbits of dominant weights μ that satisfy $\mu \prec \lambda$.*

The next lemma provides a lower bound on $\dim L(\lambda)$. The result is almost identical to [GLT12, Lemma 2.3], which is however only stated and proved for root systems of type A_r. As it turns out, a very small modification of the proof given in [GLT12] yields a uniform bound for all root systems.

Lemma 9.20. *Let $\lambda = \sum_{i=1}^{r} a_i\omega_i \in \Lambda^+$ be an ℓ-restricted weight. Then*

$$\dim L(\lambda) \geq N(\lambda) := 1 + (r+1)\left\{\prod_{i=1}^{r}\left(\left\lfloor \frac{a_i}{2} \right\rfloor + 1\right) - 1\right\}$$

Proof. Fix r integers $x_1, \ldots, x_r$ with $0 \leq x_i \leq \left\lfloor \frac{a_i}{2} \right\rfloor$. Set $\gamma := \sum x_i \alpha_i$ and let C_{ij} be the Cartan matrix of the relevant root system. By lemma 9.1, we have $\alpha_i = 2\omega_i - \sum_{j \neq i} |C_{ij}| \omega_j$ since all off-diagonal coefficients of the Cartan matrix are non-positive. It follows that the coefficient of

$$\gamma = \sum_{i=1}^{r} 2x_i\omega_i - \sum_{i=1}^{r} \sum_{j \neq i} |C_{ij}| x_i \omega_j$$

along ω_i, call it b_i, is at most $2x_i \leq a_i$. Hence $\mu := \lambda - \gamma = \sum_{i=1}^{r} (a_i - b_i)\omega_i$ is a linear combination of fundamental weights with non-negative coefficients, so it is a dominant weight. On the other hand, it is clear that $\lambda \succ \mu$, since $\lambda - \mu = \gamma$ is by construction a combination of simple roots with non-negative coefficients. Every μ thus obtained is therefore a weight of $L(\lambda)$ by Premet's theorem 9.19.

There are $\prod_{i=1}^{r} \left(\left\lfloor \frac{a_i}{2} \right\rfloor + 1 \right)$ possible choices for the integers x_i, so the module $L(\lambda)$ contains at least $\prod_{i=1}^{r} \left(\left\lfloor \frac{a_i}{2} \right\rfloor + 1 \right)$ different dominant weights, at most one of which is the zero weight. Consider now the orbits of the nonzero dominant weights under the Weyl group. Each orbit consists entirely of weights of $L(\lambda)$, and contains exactly one dominant weight. In particular, two orbits do not intersect (for otherwise we would find two Weyl-conjugated dominant weights); moreover, by lemma 9.2 the orbit of every nontrivial weight has length at least $r+1$. We have thus found at least

$$1 + (r+1) \left\{ \prod_{i=1}^{r} \left(\left\lfloor \frac{a_i}{2} \right\rfloor + 1 \right) - 1 \right\} = N(\lambda)$$

distinct weights in $L(\lambda)$, which is therefore of dimension at least $N(\lambda)$ as claimed. □

We derive in particular the following lower bound on $\dim L(\lambda)$; as we shall see below in corollary 9.29, the quantity $\sqrt{6n}$ is an upper bound for the rank of the class-$\mathcal{S}$ subgroups of $\mathrm{GSp}_{2n}(\mathbb{F}_\ell)$ of Lie type:

Proposition 9.21. *Let n be a positive integer and r be the rank of G, and suppose that r does not exceed* $\min\left\{n, \sqrt{6n}\right\}$. *If $\lambda = \sum_{i=1}^{r} a_i\omega_i \in \Lambda^+$ is an ℓ-restricted weight such that $\sum_{i=1}^{r} a_i > 2n$, then* $\dim L(\lambda) > 2n$.

Proof. The previous lemma gives $\dim L(\lambda) \geq N(\lambda) \geq 1 + (r+1)\left(\frac{1}{2}\sum_{i=1}^{r} a_i - \frac{r}{2}\right)$, where the second inequality is an equality if all but one of the a_i are equal to 1, and the remaining one is odd. It is now straightforward to check that, for $r \leq n$ and under the assumption $\sum_{i=1}^{r} a_i > 2n$, the number $1 + (r+1)\left(\frac{1}{2}\sum_{i=1}^{r} a_i - \frac{r}{2}\right)$ is not smaller than $2n+1$. □

9.6 Lifting to characteristic zero

The purpose of this section is to show that, when the characteristic ℓ is large enough (compared to n), the representation theory of subgroups of $\mathrm{GSp}_{2n}(\mathbb{F}_\ell)$ is equivalent to the representation theory of certain corresponding (algebraic) groups in characteristic zero. In order to do so, we need to ensure that the equality $L(\lambda) = V(\lambda)$ holds for all the weights λ of interest, and in view of corollary 9.18 it is enough to know that the dimension of $V(\lambda)$ is less than 2ℓ. The following lemma provides an upper bound on the dimension of Weyl modules:

Lemma 9.22. *Fix a positive integer n. Consider all simply connected, simple algebraic groups G over $\overline{\mathbb{F}_\ell}$ of rank at least 2 and at most $\min\left\{\sqrt{6n}, n\right\}$. For each such G (of rank r), consider the collection of all dominant, ℓ-restricted weights $\lambda = \sum_{i=1}^r a_i\omega_i$ such that $\sum_{i=1}^r a_i \le 2n$ and the corresponding Weyl modules $V(\lambda)$. For every such $V(\lambda)$ we have*

$$\dim V(\lambda) \le (2n+1)^{12n}.$$

Proof. Take a group G (of rank r) and a weight λ as in the statement of the lemma. Notice that any positive root α can be represented as $\alpha = \sum_{j=1}^r b_j\alpha_j$, where the b_j are non-negative integers; simple computations give $\langle\lambda,\alpha\rangle = \sum_{i=1}^r a_ib_i$ and (using the fact that $\delta = \sum_{i=1}^r \omega_i$) $\langle\delta,\alpha\rangle = \sum_{j=1}^r b_j$, so the ratio $\frac{\langle\lambda,\alpha\rangle}{\langle\delta,\alpha\rangle}$ is bounded above by $\max a_i \le \sum_{i=1}^r a_i$. By Weyl's dimension formula we have $\dim V(\lambda) = \dfrac{\prod_{\alpha\in\Delta^+}(\delta+\lambda,\alpha)}{\prod_{\alpha\in\Delta^+}(\delta,\alpha)} = \displaystyle\prod_{\alpha\in\Delta^+}\left(1+\frac{\langle\lambda,\alpha\rangle}{\langle\delta,\alpha\rangle}\right)$; combining this formula, the arithmetic-geometric inequality and the bound $\frac{\langle\lambda,\alpha\rangle}{\langle\delta,\alpha\rangle} \le \sum_{i=1}^r a_i \le 2n$ we deduce

$$\dim V(\lambda) \le \left(\frac{\sum_{\alpha\in\Delta^+}(1+\sum a_i)}{|\Delta^+|}\right)^{|\Delta^+|} \le (2n+1)^{|\Delta^+|}.$$

Finally, since the Coxeter number $h(G)$ does not exceed $4r$, we have

$$|\Delta^+| = \frac{rh(G)}{2} \le 2r^2 \le 12n,$$

and thus $\dim V(\lambda) \le (2n+1)^{12n}$ as claimed. ☐

The following proposition shows that, when the invariant q is equal to ℓ and ℓ is large enough with respect to n, every symplectic representation of dimension $2n$ comes from a corresponding representation in characteristic zero:

Proposition 9.23. *Let n be a positive integer and ℓ a prime not smaller than $\frac{1}{2}(2n+1)^{12n}$. Let G^F be a finite group as above. Suppose $\operatorname{rank}(G) \le \min\left\{\sqrt{6n}, n\right\}$ and $q = \ell$ (that is, $e = 1$). Let V be an absolutely irreducible symplectic representation of G^F over $\mathbb{F}_\ell$ of dimension $2n$. There exists an ℓ-restricted weight λ of G such that $V \otimes \overline{\mathbb{F}_\ell} = L(\lambda) \cong V(\lambda)$.*

Proof. Let r be the rank of G. We have $q = \ell$, so by theorem 9.5 $V \otimes \overline{\mathbb{F}_\ell}$ is of the form $L(\lambda)$ for a q-restricted (hence ℓ-restricted) weight λ. Write λ as $\sum_{i=1}^r a_i\omega_i$, and notice that $\sum_{i=1}^r a_i \le 2n$, for otherwise we would have $\dim V = \dim L(\lambda) > 2n$ by proposition 9.21, a contradiction. Suppose now $r \ge 2$: lemma 9.22 then gives $\dim V(\lambda) \le (2n+1)^{12n} \le 2\ell$, which by corollary 9.18 implies $L(\lambda) \cong V(\lambda)$ as desired. On the other hand, if $r = 1$ it is well-known that the equality $V(\lambda) = L(\lambda)$ holds as long as $\ell > \dim V(\lambda) = 2n$ (see for example [BHRD13, Theorem 5.3.2] and recall that $q = \ell$ in our case), and this concludes the proof of the proposition. ☐

Remark 9.24. The condition $e = 1$ in the previous preposition is automatically satisfied (corollary 9.13) as long as $2n$ is not of the form a^k with $a \ge 2$ and k an odd integer.

9.7 Order estimates

We now invoke simple order estimates to show that if the finite simple group of Lie type H appears as the socle of a class-$\mathcal{S}$ subgroup of $\mathrm{GSp}_{2n}(\mathbb{F}_\ell)$, then its rank cannot exceed $\sqrt{6n}$.

Lemma 9.25. *Let L be a finite simple group of Lie type in characteristic $\ell \neq 2,3$ and r be its rank (i.e. the rank of the corresponding algebraic group): we have $|L| \geq \ell^{r^2}$.*

Proof. The group in question is characterized by a number q (a power of ℓ) and by the family to which it belongs. For most families of simple Lie groups, the claim is easy to check by direct inspection of the explicit formulas for the orders, so let us only check families $A_r(q)$ and ${}^2A_r(q^2)$, which are arguably the least trivial ones. In the two cases, the order is given by

$$\begin{aligned}\frac{q^{r(r+1)/2}}{(r+1,q-\varepsilon)}\prod_{i=1}^{r}(q^{i+1}-\varepsilon^{i+1}) &\geq \frac{q^{r(r+1)/2}}{q(q+1)}q^{(r+1)(r+2)/2}\prod_{i=1}^{r}(1-(\varepsilon q)^{-i-1}) \\ &\geq \frac{q^{(r+1)^2}}{q(q+1)}\prod_{i=1}^{\infty}\left(1-\frac{1}{q^{i+1}}\right),\end{aligned}$$

where $\varepsilon=+1$ for $A_r(q)$ and $\varepsilon=-1$ for ${}^2A_r(q^2)$. On the other hand,

$$\log\prod_{i=1}^{\infty}(1-q^{-i-1}) = \sum_{i=1}^{\infty}\log\left(1-q^{-i-1}\right) \geq \sum_{i=1}^{\infty}-2q^{-i-1} = -\frac{2}{q(q-1)} \geq -\frac{1}{10}$$

The order of the group in question is thus at least $\exp(-1/10)\dfrac{q}{q(q+1)}q^{2r}\cdot q^{r^2} > q^{r^2} \geq \ell^{r^2}$ as claimed. ☐

We now compare this lower bound with the following upper bound due to Liebeck:

Theorem 9.26. *([Lie85, Main theorem]) Let n be a positive integer and H be a class-$\mathcal{S}$ subgroup of $\mathrm{GSp}_{2n}(\mathbb{F}_\ell)$. The order of $\mathbb{P}H$ is strictly smaller than $\max\left\{\ell^{6n},(2n+2)!\right\}$.*

Remark 9.27. The result of [Lie85] is more general, but the previous theorem suffices for our purposes.

Since $\ell^{6n} > (2n+2)!$ for $\ell > 2n+2$ we also have:

Corollary 9.28. *In the situation of the previous theorem, suppose $\ell > 2n+2$. Then the order of $\mathbb{P}H$ is strictly smaller than ℓ^{6n}.*

Corollary 9.29. *Let H be a class-$\mathcal{S}$ subgroup of $\mathrm{GSp}_{2n}(\mathbb{F}_\ell)$, with $\ell > 2n+2$. Suppose $\mathrm{soc}(\mathbb{P}H)$ is simple of Lie type in characteristic ℓ: then the rank of $\mathrm{soc}(\mathbb{P}H)$ is less than $\sqrt{6n}$.*

Proof. Indeed, if r denotes the rank of $\mathrm{soc}(\mathbb{P}H)$ we have $|\mathrm{soc}(\mathbb{P}H)| \geq \ell^{r^2}$ by lemma 9.25 and $|\mathrm{soc}(\mathbb{P}H)| < \ell^{6n}$ by corollary 9.28. ☐

9.8 The outer automorphism group

In order to reduce our study of class-$\mathcal{S}$ groups of Lie type to that of their projective socles we shall also need to have some information about the outer automorphism groups of the simple groups of Lie type.

Lemma 9.30. *Let $\ell \neq 2,3$ be a prime number. Let H be a maximal subgroup of $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$ of class $\mathcal{S}$. Suppose that $\mathrm{soc}(\mathbb{P}H) \cong G^F/Z$ is a finite simple group of Lie type in characteristic ℓ; let r be the rank of G and suppose that the invariant q attached to G^F equals ℓ. Finally, let π be the canonical projection $\mathrm{GSp}_{2g}(\mathbb{F}_\ell) \to \mathbb{P}\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$: the group $\mathrm{Out}(S)$ has exponent dividing $4(r+1)$, and for every $h \in H$ we have $\pi(h)^{4(r+1)} \in S$.*

Proof. By definition, $\mathbb{P}H$ is an almost-simple group and S is simple and normal in $\mathbb{P}H$. Recall that projective representations of G^F/Z correspond bijectively to linear representations of G^F ([Ste68, pp. 76-77, items (ix) and (x)]). We can then consider $A[\ell]$ as the linear representation of G^F that lifts the projective representation $\mathbb{P}A[\ell]$ of S and write $A[\ell] \otimes \overline{\mathbb{F}_\ell} \cong L(\lambda)$ for some integral dominant ℓ-restricted weight λ. We then obtain some information on the Lie type of G: since $q = \ell$ we are in case (1) of corollary 9.13, so the Lie type of G^F and the weight λ satisfy the conditions of corollary 9.12.

For each possible Lie type we read from [BHRD13] (and [CCN+85, p. xvi, Table 5] for the case of $E_7(\ell^e)$) the structure of $\mathrm{Out}(S)$ (cf. table 2). In most cases the exponent of these groups divides 4 (recall that $e = 1$ by hypothesis); the only exception is given by groups of type A_r and ${}^2A_r$, for which the outer automorphism group is isomorphic to a dihedral group with exponent dividing $2(r+1)$. Since 4 and $2(r+1)$ both divide $4(r+1)$, this establishes the first statement. Now notice that S is normal in $\mathbb{P}H$, whence an injection $\mathbb{P}H/S \hookrightarrow \mathrm{Out}(S)$: since the exponent of the latter group divides $4(r+1)$, we see that the exponent of $\frac{\mathbb{P}H}{S}$ divides $4(r+1)$ as well, and therefore any element $\pi(h)$ of $\mathbb{P}H$ satisfies $\pi(h)^{4(r+1)} \in S$. □

Family	Conditions	Simple group (notation as in [BHRD13])	$\mathrm{Out}(S)$
A_1		$L_2(\ell^e)$	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/e\mathbb{Z}$
A_r	$r \geq 2$	$L_{r+1}(\ell^e)$	$\mathbb{Z}/(\ell^e-1, r+1)\mathbb{Z} \rtimes \mathbb{Z}/2e\mathbb{Z}$
${}^2A_r$	$r \geq 2$	$U_{r+1}(\ell^e)$	$\mathbb{Z}/(\ell^e+1, r+1)\mathbb{Z} \rtimes \mathbb{Z}/2e\mathbb{Z}$
B_r		$O^0_{2r+1}(\ell^e)$	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/e\mathbb{Z}$
C_r		$S_{2r}(\ell^e)$	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/e\mathbb{Z}$
D_r	$r \geq 6$ even	$O^+_{2r}(\ell^e)$	$D_4 \times \mathbb{Z}/e\mathbb{Z}$
${}^2D_r$	$r \geq 4$ even	$O^-_{2r}(\ell^e)$	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2e\mathbb{Z}$
E_7		$E_7(\ell^e)$	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/e\mathbb{Z}$

Table 2: Outer automorphism groups (ℓ odd); we only include the Lie types listed in corollary 9.12.

9.9 Minuscule weights

Recall the notion of minuscule weights:

Definition 9.31. Let $\lambda \neq 0$ be a dominant integral weight for the simple group G. We say that λ is minuscule if, for every positive root α of G, we have $\langle \lambda, \alpha \rangle \in \{0, 1\}$.

Lemma 9.32. *Let λ be a dominant integral weight, α be a positive root, and $k = \langle \lambda, \alpha \rangle \in \mathbb{N}$. Every weight in the "weight string" $\lambda, \lambda - \alpha, \ldots, \lambda - k\alpha$ appears in $V(\lambda)$.*

Proof. This is well-known, see for example [Hum78, §21.3]. $\square$

Lemma 9.33. *Let $\lambda \neq 0$ be a dominant integral weight of G which is not minuscule, and let $\rho : G \to \mathrm{GL}_{V(\lambda)}$ be the corresponding irreducible representation. For every $x \in G(\overline{\mathbb{F}_\ell})$ there are three eigenvalues $\lambda_1, \lambda_2, \lambda_3$ of $\rho(x)$ that satisfy $\lambda_2^2 = \lambda_1\lambda_3$.*

Proof. By assumption λ is not minuscule, hence there exists a positive root α such that $\langle \lambda, \alpha \rangle = k \geq 2$. By lemma 9.32, the three weights $w_1 = \lambda, w_2 = \lambda - \alpha, w_3 = \lambda - 2\alpha$ all appear in $V(\lambda)$, and they satisfy the equation $2w_2 = w_1 + w_3$. This concludes the proof, because by definition of weight for all $x \in G(\overline{\mathbb{F}_\ell})$ the operator $\rho(x)$ possesses the three eigenvalues $w_1(x), w_2(x), w_3(x)$, which satisfy $w_2(x)^2 = w_1(x)w_3(x)$. $\square$

9.10 Conclusion: the non-minuscule case, $e = 1$

Recall our notation from the introduction: we consider an abelian variety A/K such that $\mathrm{End}_{\overline{K}}(A) = \mathbb{Z}$, and we fix a place v of K, of good reduction for A, such that the characteristic polynomial $f_v(x)$ of the Frobenius at v has Galois group isomorphic to $(\mathbb{Z}/2\mathbb{Z})^g \rtimes S_g$. We now prove that, for ℓ large enough, G_ℓ is not contained in a maximal subgroup of $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$ of class $\mathcal{S}$ that satisfies the following conditions:

1. the projective socle $S = G^F/Z$ of the maximal subgroup in question is of Lie type in characteristic ℓ;
2. the invariant q attached to S is equal to ℓ;
3. the representation $A[\ell]$ of G^F obtained by lifting the projective representation $\mathbb{P}A[\ell]$ of S is defined by a non-minuscule weight.

Proposition 9.34. *Let ℓ be a prime as in assumption 2.5. Let v be a place of K at which A has good reduction, and suppose that $f_v(x)$ has Galois group $(\mathbb{Z}/2\mathbb{Z})^g \rtimes S_g$. Suppose that ℓ is strictly larger than $\left(2q_v^{4(\sqrt{6g}+1)}\right)^{[F(v):\mathbb{Q}]}$. The group G_ℓ is not contained in a maximal subgroup of class $\mathcal{S}$ that satisfies conditions 1, 2 and 3 above.*

Proof. Suppose by contradiction that G_ℓ *is* contained in such a maximal subgroup H. With the notation of the previous paragraphs, write the finite simple group $\mathrm{soc}\,\mathbb{P}H$ as G^F/Z (with associated algebraic data G, q). As already mentioned, projective representations of G^F/Z correspond bijectively to linear representations of G^F, and furthermore, by definition of class $\mathcal{S}$, the representation $A[\ell]$ of G^F is absolutely irreducible. Notice now that we can apply proposition 9.23: indeed the inequality $r \leq \sqrt{6g}$ follows from corollary 9.29 (the tables of [BHRD13] show that when $g < 7$ there are no exceptional class-$\mathcal{S}$ subgroups of Lie type except those with socle $\mathrm{PSL}_2(\mathbb{F}_\ell)$, so we can assume $\min\{g, \sqrt{6g}\} = \sqrt{6g}$). We can in particular write $A[\ell] \otimes \overline{\mathbb{F}_\ell} \cong L(\lambda) \cong V(\lambda)$ for some ℓ-restricted weight λ. The following commutative diagram summarizes the situation:

$$
\begin{tikzcd}
\mathrm{Gal}\left(\overline{K}/K\right) \arrow[dr, "\rho_\ell"] \arrow[ddr, bend right, "\pi\circ\rho_\ell"'] & \mathrm{Aut}\, V(\lambda) & G\left(\overline{\mathbb{F}_\ell}\right) \arrow[l, hook', "\rho_{V(\lambda)}"'] \\
& \mathrm{Aut}\, A[\ell] \arrow[u, hook] \arrow[d, "\pi"] & G^F \arrow[l, "\rho"] \arrow[u, hook] \arrow[dl, bend left, "\pi\circ\rho"] \\
& \mathbb{P}\, \mathrm{Aut}\, A[\ell] &
\end{tikzcd}
$$

where $\mathrm{soc}\,(\mathbb{P}H) = \mathrm{Im}(\pi \circ \rho)$. In particular, since by assumption $G_\ell \subseteq H$, it follows from lemma 9.30 that for every $y \in \mathrm{Gal}\left(\overline{K}/K\right)$ there exist $\mu \in \mathbb{F}_\ell^\times$ and $x \in G^F \subseteq G\left(\overline{\mathbb{F}_\ell}\right)$ such that

$$\rho_\ell(y)^{4(r+1)} = \mu\rho(x),$$

and therefore the eigenvalues of $\rho_\ell(y)^{4(r+1)}$ are given by $\{\mu\lambda_1, \dots, \mu\lambda_{2g}\}$, where $\lambda_1, \dots, \lambda_{2g}$ are the eigenvalues of $\rho(x)$. Now recall that by assumption the weight λ is not minuscule. Up to renumbering the λ_i, we then see from lemma 9.33 that we have $\lambda_2^2 = \lambda_1\lambda_3$, and therefore $(\mu\lambda_2)^{8(r+1)} = (\mu\lambda_1)^{4(r+1)}(\mu\lambda_3)^{4(r+1)}$. We have thus proved that for every $y \in \mathrm{Gal}\left(\overline{K}/K\right)$ the operator $\rho_\ell(y)$ has three eigenvalues $\mu_1, \mu_2, \mu_3 \in \overline{\mathbb{F}_\ell}^\times$ that satisfy

$$\mu_2^{8(r+1)} = \mu_1^{4(r+1)} \cdot \mu_3^{4(r+1)} \text{ in } \overline{\mathbb{F}_\ell}. \tag{6}$$

Now apply this to $y = \mathrm{Fr}_v$: the polynomial $f_v(x)$ has three roots $\mu_1, \mu_2, \mu_3 \in \overline{\mathbb{Q}}^\times$ that (when regarded in $\overline{\mathbb{F}_\ell}$) satisfy equation (6). Recall that we denote by $F(v)$ the splitting field of $f_v(x)$, and that the Galois group of $f_v(x)$ is $(\mathbb{Z}/2\mathbb{Z})^g \rtimes S_g$ by assumption. We distinguish two cases:

- $\mu_1 = \iota(\mu_3)$. Since $\mu_3\iota(\mu_3) = q_v$, this implies $\overline{\mu_2}^{8(r+1)} - q_v^{4(r+1)} = 0$ in $\overline{\mathbb{F}_\ell}$; on the other hand, μ_2 is *not* a root of the polynomial $x^{8(r+1)} - q_v^{4(r+1)} \in \mathbb{Z}[x]$ (lemma 2.9), so $\mu_2^{8(r+1)} - q_v^{4(r+1)}$ is nonzero.

  We now proceed as in section 7: the equality $\overline{\mu_2}^{8(r+1)} - q_v^{4(r+1)} = 0 \in \overline{\mathbb{F}_\ell}$ shows that ℓ divides the nonzero integer $\left|N_{F(v)/\mathbb{Q}}\left(\mu_2^{8(r+1)} - q_v^{4(r+1)}\right)\right|$, and the Weil conjectures imply that $\left|N_{F(v)/\mathbb{Q}}\left(\mu_2^{8(r+1)} - q_v^{4(r+1)}\right)\right|$ does not exceed $\left(2q_v^{4(r+1)}\right)^{[F(v):\mathbb{Q}]}$, so we must have $\ell \leq \left(2q_v^{4(r+1)}\right)^{[F(v):\mathbb{Q}]}$.

- $\mu_1 = \iota(\mu_2)$ or $\mu_1 \neq \iota(\mu_2), \iota(\mu_3)$. By lemma 2.8 we cannot have $\mu_2^{8(r+1)} = \mu_1^{4(r+1)}\mu_3^{4(r+1)}$ in $\overline{\mathbb{Q}}^\times$. We then reason as in the previous case: the algebraic integer $\mu_2^{8(r+1)} - \mu_1^{4(r+1)}\mu_3^{4(r+1)}$ is nonzero and ℓ divides its norm, so the inequality $\ell \leq \left(2q_v^{4(r+1)}\right)^{[F(v):\mathbb{Q}]}$ must hold.

Taking into account the inequality $r \leq \sqrt{6g}$, in all cases we have reached a contradiction with our assumption $\ell > \left(2q_v^{4(\sqrt{6g}+1)}\right)^{[F(v):\mathbb{Q}]}$, and the proposition is proved. $\square$

9.11 Conclusion: the minuscule case, $e = 1$

In this section we consider the case of subgroups of class $\mathcal{S}$ acting through representations defined by minuscule weights. Once more we fix a place v of K such that A has good reduction at v and the characteristic polynomial $f_v(x)$ of Fr_v has Galois group isomorphic to $(\mathbb{Z}/2\mathbb{Z})^g \rtimes S_g$.

We start by describing a sufficient criterion that, given a finite simple group of Lie type S, with $S \cong G^F/Z$, and a minuscule weight of the algebraic group G, ensures that G_ℓ is *not* contained in a maximal subgroup of $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$ of class $\mathcal{S}$, with projective socle S acting on $\mathbb{P}A[\ell]$ through the projectivization of the representation corresponding to the given minuscule weight. Given the very limited number of minuscule weights, it will then be easy to check by hand that this criterion applies to every minuscule weight that gives rise to a symplectic representation.

Suppose then that G_ℓ is contained in a maximal subgroup G of $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$ with projective socle S (a finite simple group of Lie type in characteristic ℓ), and suppose furthermore that the invariant q attached to S is equal to ℓ (so that, in the notation of the previous paragraphs, we have $e = 1$). Let G^F be the universal central extension of S, and suppose that $A[\ell]$ (considered as the representation of G^F that lifts the projective representation $\mathbb{P}A[\ell]$ of S), is defined by the highest weight λ. We shall only be interested in primes larger than $(2q_v^{4(\sqrt{6g}+1)})^{2^g g!}$, so (applying proposition 9.23 and taking into account corollary 9.29) we know that $V(\lambda) \cong L(\lambda)$ for all the primes we are interested in.

Let $\lambda_1, \ldots, \lambda_{2g}$ be the weights appearing in $A[\ell]$ (again as a representation of G^F), and let N be the exponent of $\operatorname{Out} S$. Suppose that (up to renumbering the weights $\lambda_1, \ldots, \lambda_{2g}$) we have $\lambda_1 + \cdots + \lambda_n = \lambda_{n+1} + \cdots + \lambda_{2n}$ for some odd n. Then, for every $[s] \in S$ and every lift s of $[s]$ in $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$, the operator s admits $2n$ eigenvalues $\overline{\mu_1}, \ldots, \overline{\mu_{2n}}$ that satisfy $\overline{\mu_1} \cdots \overline{\mu_n} = \overline{\mu_{n+1}} \cdots \overline{\mu_{2n}}$. Conversely, given any $h \in G_\ell$, its projective image $[h]$ satisfies $[h]^N \in S$, so (setting $[s] = [h]^N$ and $s = h^N$) we see that h^N has $2n$ eigenvalues that satisfy the previous equation. Since the eigenvalues of s are the N-th powers of the eigenvalues of h, we deduce that every operator $h \in G_\ell$ has $2n$ eigenvalues $\overline{\mu_1}, \ldots, \overline{\mu_{2n}}$ that satisfy

$$\overline{\mu_1}^N \cdots \overline{\mu_n}^N = \overline{\mu_{n+1}}^N \cdots \overline{\mu_{2n}}^N \text{ in } \overline{\mathbb{F}_\ell}. \tag{7}$$

Specialize now this discussion to $h = \rho_\ell(\mathrm{Fr}_v)$. For this choice of h there are $2n$ eigenvalues of Fr_v, call them $\mu_1, \ldots, \mu_{2n}$, whose reductions in $\overline{\mathbb{F}_\ell}$ satisfy equation (7). However, by corollary 2.11 we know that $(\mu_1 \cdots \mu_n)^N - (\mu_{n+1} \cdots \mu_{2n})^N$ is nonzero, so (as we did in section 7 and in the proof of proposition 9.34) we deduce that ℓ divides the nonzero integer $|N_{F(v)/\mathbb{Q}}\left(\mu_1^N \cdots \mu_n^N - \mu_{n+1}^N \cdots \mu_{2n}^N\right)|$, and by the Weil conjectures this integer does not exceed $(2q_v^{nN/2})^{[F(v):\mathbb{Q}]}$. We have proved:

Lemma 9.35. *Suppose that G_ℓ is contained in a maximal subgroup of class $\mathcal{S}$ having projective socle $S = G^F/Z$. Consider $A[\ell]$ as the linear representation of G^F that lifts the projective representation $\mathbb{P}A[\ell]$ of S, and let $\lambda_1, \ldots, \lambda_{2g}$ be the weights of this representation. Suppose we can find an odd integer n such that (up to renumbering) the weights $\lambda_1, \ldots, \lambda_{2g}$ satisfy*

$$\lambda_1 + \cdots + \lambda_n = \lambda_{n+1} + \cdots + \lambda_{2n}.$$

Finally let N be the exponent of the outer automorphism group of S. Then the inequality $\ell \leq (2q_v^{nN/2})^{[F(v):\mathbb{Q}]}$ holds.

Proposition 9.36. *Suppose that G_ℓ is contained in a maximal class-$\mathcal{S}$ subgroup with projective socle S of Lie type in characteristic ℓ. Suppose furthermore that the invariant q attached to S is equal to ℓ. Then the inequality $\ell \leq (2q_v^{4(\sqrt{6g}+1)})^{2^g g!}$ holds.*

Proof. Thanks to the result of proposition 9.34, this is true if the projective socle acts on $\mathbb{P}A[\ell]$ through a non-minuscule weight. We treat the case of minuscule weights in the next few subsections. □

We now consider the explicit list of minuscule weights that give rise to symplectic representations. Let G be of rank r, and suppose we realize its root system in the Euclidean vector space $\mathbb{R}^r$ as described in [Bou02, Planches I-IX]. Then $\varepsilon_1, \ldots, \varepsilon_r$ are a basis of $\mathbb{R}^r$, and we can express the simple roots of G and its fundamental weights in terms of $\varepsilon_1, \ldots, \varepsilon_r$. Notice that if ω is a positive dominant integral weight that is also minuscule, then the set of weights appearing in $V(\lambda)$ (hence in $L(\lambda)$) is given precisely by the orbit of ω under the Weyl group $W(G)$, cf. [Bou08, §8.3, Proposition 6]. Furthermore, a description of the action of $W(G)$ on $\varepsilon_1, \ldots, \varepsilon_r$ can be read off [Bou02, Planches I-IX]. We shall make use of this information without further reference to [Bou02].

9.11.1 Lie type A_r, $r \equiv 1 \pmod 4$

When $r \not\equiv 1 \pmod 4$ there are no minuscule representations that are symplectic. On the other hand, when $r \equiv 1 \pmod 4$, the only minuscule weight giving rise to a symplectic representation is $\varpi_{(r+1)/2} = \sum_{i=1}^{(r+1)/2} \varepsilon_i - \frac{1}{2}\sum_{i=(r+3)/2}^{r+1} \varepsilon_i$. Notice that when $r = 1$ this corresponds to the standard representation of SL_2, of dimension 2, which can only happen for $g = 1$, a case that does not interest us. We can therefore assume $r \geq 5$. The Weyl group of A_r is S_{r+1}, acting naturally on the ε_i by permutation. It follows that the weights appearing in $L(\varpi_{(r+1)/2}) = V(\varpi_{(r+1)/2})$ are precisely those of the form $\sum_{i=1}^{r+1} a_i \varepsilon_i$, where for $(r+1)/2$ indices i we have $a_i = 1$, and for the remaining $(r+1)/2$ indices we have $a_i = -1/2$. In particular, we can consider the following weights: set $\omega = \displaystyle\sum_{i=7}^{\frac{r+7}{2}} \varepsilon_i - \frac{1}{2}\sum_{i=\frac{r+9}{2}}^{r+1} \varepsilon_i$ (where $\omega = 0$ if $r = 5$) and

$$\begin{aligned}
\lambda_1 &= -\frac{1}{2}\varepsilon_1 + \varepsilon_2 + \varepsilon_3 + \varepsilon_4 - \frac{1}{2}\varepsilon_5 - \frac{1}{2}\varepsilon_6 + \omega\\
\lambda_2 &= +\varepsilon_1 - \frac{1}{2}\varepsilon_2 + \varepsilon_3 - \frac{1}{2}\varepsilon_4 + \varepsilon_5 - \frac{1}{2}\varepsilon_6 + \omega\\
\lambda_3 &= +\varepsilon_1 + \varepsilon_2 - \frac{1}{2}\varepsilon_3 - \frac{1}{2}\varepsilon_4 - \frac{1}{2}\varepsilon_5 + \varepsilon_6 + \omega\\
\lambda_4 &= +\varepsilon_1 + \varepsilon_2 - \frac{1}{2}\varepsilon_3 + \varepsilon_4 - \frac{1}{2}\varepsilon_5 - \frac{1}{2}\varepsilon_6 + \omega\\
\lambda_5 &= -\frac{1}{2}\varepsilon_1 + \varepsilon_2 + \varepsilon_3 - \frac{1}{2}\varepsilon_4 + \varepsilon_5 - \frac{1}{2}\varepsilon_6 + \omega\\
\lambda_6 &= +\varepsilon_1 - \frac{1}{2}\varepsilon_2 + \varepsilon_3 - \frac{1}{2}\varepsilon_4 - \frac{1}{2}\varepsilon_5 + \varepsilon_6 + \omega
\end{aligned}$$

It is immediate to check that $\lambda_1, \ldots, \lambda_6$ are all distinct and that $\lambda_1 + \lambda_2 + \lambda_3 = \lambda_4 + \lambda_5 + \lambda_6$. Furthermore, if $A[\ell]$ is a symplectic minuscule representation of G^F and G is of Lie type type A_r, then $2g = \dim A[\ell] = \binom{r+1}{(r+1)/2} \geq 2^r$; finally, the exponent of the outer automorphism group of a finite simple group of Lie type A_r divides $2(r+1)$. Using lemma 9.35 we thus

see that if G_ℓ is contained in a maximal class-$\mathcal{S}$ subgroup with projective socle $S = G^F/Z$ of Lie type A_r ($r \equiv 1 \pmod 4$), and if furthermore $A[\ell]$ is isomorphic to $V(\varpi_{(r+1)/2})$ as a representation of G^F, then $\ell \leq \left(2q_v^{3(r+1)}\right)^{[F(v):\mathbb{Q}]}$. Using the inequality $r \leq 1 + \log_2(g)$ we conclude that for $\ell > (2q_v^{4(\sqrt{6g}+1)})^{2^g g!}$ the group G_ℓ cannot be contained in a maximal class-$\mathcal{S}$ subgroup with projective socle of Lie type A_r.

9.11.2 Lie type B_r, $r \equiv 1, 2 \pmod 4$

The only minuscule, symplectic representation is $V(\varpi_r)$, where $\varpi_r = \frac{1}{2}\sum_{i=1}^r \varepsilon_i$. This representation is of dimension 2^r, so since we are assuming that $A[\ell] \otimes \overline{\mathbb{F}_\ell} \cong V(\varpi_r)$ we must have $2g = 2^r$. If $r \leq 2$ we find $g \leq 2$, a case which does not interest us; we can thus assume $r \geq 5$. The Weyl group is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^r \rtimes S_r$, with the factor S_r acting on the ε_i by permutation, while the nontrivial element in the i-th factor $\mathbb{Z}/2\mathbb{Z}$ acts on ε_i by sending it to $-\varepsilon_i$. We apply our criterion with $\lambda_1 = \frac{1}{2}(1, 1, 1, 1, 1, \underbrace{1, \ldots, 1}_{r-5})$, $\lambda_2 = \frac{1}{2}(-1, -1, -1, -1, -1, \underbrace{1, \ldots, 1}_{r-5})$, $\lambda_3 = \frac{1}{2}(1, 1, 1, 1, -1, \underbrace{1, \ldots, 1}_{r-5})$, $\lambda_4 = \frac{1}{2}(1, -1, 1, -1, 1, \underbrace{1, \ldots, 1}_{r-5})$, $\lambda_5 = \frac{1}{2}(1, 1, -1, 1, -1, \underbrace{1, \ldots, 1}_{r-5})$ and $\lambda_6 = \frac{1}{2}(-1, 1, 1, 1, -1, \underbrace{1, \ldots, 1}_{r-5})$, where we write weights as the vectors of their coordinates in the basis of the ε_i. Since $\dim V(\varpi_r) = 2^r$ one obtains $r = 1 + \log_2(g)$, and as above we conclude that G_ℓ cannot be contained in a maximal class-$\mathcal{S}$ subgroup with projective socle of Lie type B_r as long as $\ell > (2q_v^{4(\sqrt{6g}+1)})^{2^g g!}$.

9.11.3 Lie type C_r, $r \geq 3$

The only minuscule, symplectic module for a group of type C_r is the defining representation $V(\varpi_1)$, of dimension $2r$ (so $r = g$). This representation clearly does not give rise to a maximal class-$\mathcal{S}$ subgroup of $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$.

9.11.4 Lie type D_r, $r \equiv 2 \pmod 4$, $r \geq 6$

This is perfectly analogous to the case of B_r. The only two minuscule, symplectic representations are associated with the weights $\varpi_{r-1} = \frac{1}{2}\sum_{i=1}^{r-1} \varepsilon_i - \frac{1}{2}\varepsilon_r$ and $\varpi_r = \frac{1}{2}\sum_{i=1}^r \varepsilon_i$. The Weyl group is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^{r-1} \rtimes S_r$, where the factor S_r acts by permutation on the ε_i while the factor $(\mathbb{Z}/2\mathbb{Z})^{r-1} \cong \left\{(e_1, \ldots, e_r) \in (\pm 1)^r \;\middle|\; \prod_{i=1}^r e_r = 1\right\}$ acts by the formula $(e_1, \ldots, e_r) \cdot \sum_{i=1}^r a_i\varepsilon_i = \sum_{i=1}^r e_i a_i \varepsilon_i$. Again we write weights as the vectors of their

coordinates in the basis ε_i; for the representation $V(\varpi_r)$ we can take

$$\lambda_1 = \frac{1}{2}(1,1,1,1,1,1,\underbrace{1,\dots,1}_{r-6})$$

$$\lambda_2 = \frac{1}{2}(-1,-1,-1,1,-1,1,\underbrace{1,\dots,1}_{r-6})$$

$$\lambda_3 = \frac{1}{2}(1,1,1,-1,1,-1,\underbrace{1,\dots,1}_{r-6})$$

$$\lambda_4 = \frac{1}{2}(-1,-1,1,1,1,1,\underbrace{1,\dots,1}_{r-6})$$

$$\lambda_5 = \frac{1}{2}(1,1,-1,-1,1,1,\underbrace{1,\dots,1}_{r-6})$$

$$\lambda_6 = \frac{1}{2}(1,1,1,1,-1,-1,\underbrace{1,\dots,1}_{r-6}).$$

For the representation $V(\varpi_{r-1})$ it suffices to change the sign of the sixth coordinates of the vectors just listed. Since $V(\varpi_{r-1})$, $V(\varpi_r)$ are the half-spin representations, of dimension 2^{r-1}, we obtain $r = \log_2(g) + 2 < \sqrt{6g} + 1$; we deduce easily that for $\ell > (2q_v^{4(\sqrt{6g}+1)})^{2^g g!}$ the group G_ℓ cannot be contained in a maximal class-$\mathcal{S}$ subgroup with projective socle of Lie type D_r.

9.11.5 Lie type E_7

The only minuscule weight giving rise to a symplectic representation is $\varpi_7 = \varepsilon_6 + \frac{1}{2}(\varepsilon_8 - \varepsilon_7)$. The representation is 56-dimensional, so this case can only arise when $g = 28$. It is not hard to check that for any choice of $(e_1,\dots,e_6) \in (\pm 1)^6$ such that $\prod_{i=1}^6 e_i = 1$ the weight $\frac{1}{2}\sum_{i=1}^6 e_i\varepsilon_i$ appears in $V(\varpi_7)$; we can then apply our criterion with the following six weights:

$$\lambda_1 = \frac{1}{2}(1,1,1,1,1,1,0,0)$$
$$\lambda_2 = \frac{1}{2}(-1,-1,-1,1,-1,1,0,0)$$
$$\lambda_3 = \frac{1}{2}(1,1,1,-1,1,-1,0,0)$$
$$\lambda_4 = \frac{1}{2}(-1,-1,1,1,1,1,0,0)$$
$$\lambda_5 = \frac{1}{2}(1,1,-1,-1,1,1,0,0)$$
$$\lambda_6 = \frac{1}{2}(1,1,1,1,-1,-1,0,0).$$

In this case we know the rank to be $r = 7$, while the outer automorphism group has order (hence exponent) 2. We conclude once more that for $\ell > (2q_v^{4(\sqrt{6g}+1)})^{2^g g!}$ the group G_ℓ cannot be contained in a maximal class-$\mathcal{S}$ subgroup with projective socle of Lie type E_7.

9.12 Conclusion: case $e > 1$

To completely rule out the maximal subgroups of class $\mathcal{S}$ the last possibility we need to consider is case (2) in corollary 9.13. More precisely, we now consider the case of G_ℓ being contained in a maximal class-$\mathcal{S}$ subgroup of $\operatorname{GSp}_{2g}(\mathbb{F}_\ell)$ whose projective socle $S = G^F/Z$ has invariant $q = \ell^e$ with $e > 1$. We shall only need the fact that in this case $A[\ell] \otimes \overline{\mathbb{F}_\ell}$ is tensor-decomposable under the action of G^F, as proved in corollary 9.13. We start with an upper bound for the exponent of $\operatorname{Out}(S)$:

Lemma 9.37. *The exponent of the group* $\operatorname{Out}(S)$ *does not exceed* $4\sqrt{6g}$.

Proof. By table 2 the exponent does not exceed $2e(r+1)$ (where r is the rank of G), and since $\dim A[\ell] = 2g$ is a perfect e-th power by corollary 9.13 we find $e \leq \log_2(2g)$. Moreover, from the proof of corollary 9.13 we see that the algebraic group G admits a nontrivial irreducible representation of dimension $(2g)^{1/e}$, so its rank is at most $(2g)^{1/e} - 1$ (notice that a nontrivial irreducible representation of dimension n induces a nontrivial map $G \to \operatorname{SL}_n$, which in turn implies $r = \operatorname{rk} G \leq \operatorname{rk} \operatorname{SL}_n = n-1$). Finally, using $e \geq 3$ (hence $g \geq 4$) one easily finds that $2e(r+1) \leq 2\log_2(2g)(2g)^{1/3} \leq 4\sqrt{6g}$. ∎

Proposition 9.38. *Let ℓ be a prime as in assumption 2.5. Suppose that G_ℓ is contained in a maximal class-$\mathcal{S}$ subgroup H of $\operatorname{GSp}_{2g}(\mathbb{F}_\ell)$ such that $S = \operatorname{soc}(\mathbb{P}H)$ of Lie type in characteristic ℓ. Suppose furthermore that $S = G^F/Z$ has invariant $q = \ell^e$ with $e > 1$. Then* $\ell \leq (2q_v^{4(\sqrt{6g}+1)})^{2^g g!}$

Proof. Assume by contradiction that $\ell > (2q_v^{4(\sqrt{6g}+1)})^{2^g g!}$ and that G_ℓ is contained in a maximal subgroup of class $\mathcal{S}$ as in the statement of the proposition. As in the previous sections, we aim to reach a contradiction by writing down a polynomial relation with small exponents satisfied by the eigenvalues of the elements of $\rho_\ell(\operatorname{Fr}_v)$.

Let N be the exponent of $\operatorname{Out}(S)$. Since $\mathbb{P}H/S$ embeds into $\operatorname{Out} S$, we see that for every $h \in H$ we have $[h^N] \in S$. By corollary 9.13 we know that $A[\ell] \otimes \overline{\mathbb{F}_\ell}$, considered as a representation of G^F, is tensor-decomposable in precisely e factors. Write $2g = (2m)^e$. It follows that there exist $g'_1, \ldots, g'_e \in \operatorname{GSp}_{2m}(\overline{\mathbb{F}_\ell})$ such that

$$h^N = h'_1 \otimes \cdots \otimes h'_e.$$

Now the eigenvalues h^N are of the form $\lambda_1 \cdots \lambda_e$, where every λ_i ranges over the eigenvalues of h'_i. We write $\{\lambda_{i,j} \bigm| j = 1, \ldots, 2m\}$ for the multiset of eigenvalues of h'_i.

Let us now specialize this discussion to $h = \rho_\ell(\operatorname{Fr}_v)$, so that the eigenvalues $\overline{\mu_1}, \ldots, \overline{\mu_{2g}}$ of h can be recovered as the reduction in $\overline{\mathbb{F}_\ell}$ of the eigenvalues $\mu_1, \ldots, \mu_{2g}$ of Fr_v. Notice that the inequality $\ell > (2q_v^{4(\sqrt{6g}+1)})^{2^g g!}$ implies that $\overline{\mu_1}, \ldots, \overline{\mu_{2g}}$ are all distinct: if we had $\overline{\mu_i} = \overline{\mu_j}$ for some $i \neq j$, then ℓ would divide the nonzero integer $|N_{F(v)/\mathbb{Q}}(\mu_i - \mu_j)| \leq \left(2q_v^{1/2}\right)^{[F(v):\mathbb{Q}]}$, contradiction.

Up to renumbering, we can assume that for all $i = 1, \ldots, 2g$ the algebraic integers μ_{2g+1-i} and μ_i are complex conjugates to each other. Let $x_1 = \overline{\mu_1}^N, \ldots, x_{2g} = \overline{\mu_{2g}}^N$ be the eigenvalues of h^N. The same argument as above ensures that the x_i are all distinct: if we had $x_i = x_j$ for some $i \neq j$, then ℓ would divide $|N_{F(v)/\mathbb{Q}}(\mu_i^N - \mu_j^N)| \leq \left(2q_v^{N/2}\right)^{[F(v):\mathbb{Q}]}$, contradiction (notice that $\mu_i^N \neq \mu_j^N$ by corollary 2.11). Furthermore, up to renumbering the $\lambda_{i,j}$ we can assume that $x_1 = \prod_{i=1}^t \lambda_{i,1}$.

For every index $k = 1, \ldots, 2g$ fix now a function $j_k(i) : \{1, \ldots, e\} \to \{1, \ldots, 2m\}$ such that $x_k = \prod_{i=1}^e \lambda_{i, j_k(i)}$. Notice that since the x_i are all distinct so must be the functions $j_k(i)$; as there are $(2m)^e$ possible functions and $2g = (2m)^e$ eigenvalues, it follows that every eigenvalue corresponds to precisely one function, and clearly every function is realized by an eigenvalue.

We claim that there is an index $k \in \{2, \ldots, g\}$ such that $j_k(i)$ takes values different from 1 at least twice (that is to say, there exist $k \in \{2, \ldots, g\}$ and $i_1, i_2 \in \{1, \ldots, e\}$ such that $j_k(i_1) \neq 1$, $j_k(i_2) \neq 1$). Suppose by contradiction that this is not the case. Then there are at most $1 + e(2m-1)$ possible functions $j_k(i)$ representing the eigenvalues $x_1, \ldots, x_g$ (the constant function 1, and those that differ by it at precisely one spot), and since no function can appear more than once we deduce in particular $1 + e(2m-1) \geq g$. However by definition we have $g = 2^{e-1} m^e = 2^{e-1}(1 + (m-1))^e \geq 4(1 + e(m-1))$, a contradiction to what we just proved, and this establishes our claim. Also notice that the eigenvalue $x_k = \overline{\mu_k}^N$ is the reduction in $\overline{\mathbb{F}_\ell}$ of μ_k^N, and μ_k is not the complex conjugate of μ_1, because $k \leq g$ and the complex conjugate of μ_1 is μ_{2g}. We shall need this information presently.

Let now k, i_1, i_2 be indices as in the previous paragraph. Consider the four (distinct) functions

$$e_1(i) = 1, \quad e_2(i) = j_k(i), \quad e_3(i) = \begin{cases} 1, \text{ if } i \neq i_1 \\ j_k(i_1), \text{ if } i = i_1 \end{cases}, \quad e_4(i) = \begin{cases} 1, \text{ if } i \neq i_2 \\ j_k(i_2), \text{ if } i = i_2 \end{cases}$$

and the four eigenvalues $y_j = \prod_{i=1}^e \lambda_{i, e_j(i)}$ (for $j = 1, \ldots, 4$) of h^N. By construction we have $y_1 y_2 = y_3 y_4$, and up to renumbering once more we can assume that $y_j = \overline{\mu_j}^N$ for $j = 1, 2, 3, 4$. It follows that ℓ divides $N_{F(v)/\mathbb{Q}}(\mu_1^N \mu_2^N - \mu_3^N \mu_4^N)$. Notice now that $\mu_1^N \mu_2^N - \mu_3^N \mu_4^N$ is nonzero (this follows from lemma 2.8 and the fact that μ_2, as we already noticed, is not the complex conjugate of μ_1), so by an argument we have used many times we find $\ell \leq \left(2q_v^N\right)^{[F(v):\mathbb{Q}]}$. Using the inequality $N < 4(\sqrt{6g} + 1)$ we reach a contradiction, and the proposition is proved. □

10 Tensor induced subgroups

We come to the case of tensor induced subgroups $\mathrm{GSp}_{2m}(\mathbb{F}_\ell) \wr S_t$, where $2g = (2m)^t$. The arguments and the results we need are very close to those of section 9.12, so we fix from the start a place v of K, of good reduction for A, such that the characteristic polynomial $f_v(x)$ of the Frobenius at v has Galois group $(\mathbb{Z}/2\mathbb{Z})^g \rtimes S_g$. We also keep the notation Φ_v for the set of roots of $f_v(x)$. We shall need the following result:

Theorem 10.1. *([MNR89, Theorem 2]) Let* $\xi(n) = \max_{\sigma \in S_n} \operatorname{order}(\sigma)$. *For all* $n \geq 3$ *we have*

$$\xi(n) \leq \exp\left(\sqrt{n \log n}\left(1 + \frac{\log\log n - 0.975}{2 \log n}\right)\right).$$

Proposition 10.2. *Let* v *be a place of* K *of good reduction for* A *such that the Galois group of the characteristic polynomial* $f_v(x)$ *is* $(\mathbb{Z}/2\mathbb{Z})^g \rtimes S_g$. *Let* ℓ *be a prime as in assumption 2.5, and suppose* $\ell > (2q_v^{4(\sqrt{6g}+1)})^{2^g g!}$. *The group* G_ℓ *is not contained in a tensor induced subgroup* $\mathrm{GSp}_{2m}(\mathbb{F}_\ell) \wr S_t$, *where* $m \geq 1, t \geq 3$ *are integers such that* $(2m)^t = 2g$.

Proof. The proof is very similar to that of proposition 9.38. Assume by contradiction that $\ell > (2q_v^{4(\sqrt{6g}+1)})^{2^g g!}$ and that G_ℓ is contained in a tensor induced group $\mathrm{GSp}_{2m}(\mathbb{F}_\ell) \wr S_t$. Once again, we shall reach a contradiction by writing down a polynomial relation with small exponents satisfied by the eigenvalues of the elements of $\mathrm{GSp}_{2m}(\mathbb{F}_\ell) \wr S_t$.

To get rid of the symmetric group S_t, notice first that by definition we have $2g = (2m)^t$, so $t = \log_{2m}(2g) \leq \log_2(2g)$ and the order of a permutation in S_t does not exceed

$$\xi(t) \leq \xi(\log_2(2g)) < 4(\sqrt{6g} + 1).$$

We represent an element $h \in G_\ell \subseteq \mathrm{GSp}_{2m}(\mathbb{F}_\ell) \wr S_t$ as a pair $(g_1 \otimes \cdots \otimes g_t, \sigma)$, where $g_1, \ldots, g_t$ are in $\mathrm{GSp}_{2m}(\mathbb{F}_\ell)$ and σ is a permutation in S_t. Let a be the order of σ; by what we just saw, a does not exceed $4(\sqrt{6g} + 1)$. In particular, for every $h \in G_\ell$ there exist $a \in \mathbb{N}$, $a \leq 4(\sqrt{6g} + 1)$, and $g_1', \ldots, g_t' \in \mathrm{GSp}_{2m}(\mathbb{F}_\ell)$ such that

$$h^a = \left(g_1' \otimes \cdots \otimes g_t', \mathrm{Id}\right).$$

We now proceed exactly as in the proof of proposition 9.38: we take $h = \rho_\ell(\mathrm{Fr}_v)$ and write $\mu_1, \ldots, \mu_{2g}$ for the roots of the characteristic polynomial $f_v(x)$. We easily find that h^a has four distinct eigenvalues $\overline{\mu_1}^a, \overline{\mu_2}^a, \overline{\mu_3}^a, \overline{\mu_4}^a$ that satisfy $\overline{\mu_1}^a \overline{\mu_2}^a = \overline{\mu_3}^a \overline{\mu_4}^a$ and are such that $\mu_2 \neq \iota(\mu_1)$. From lemma 2.8 and the fact that μ_2 is not the complex conjugate of μ_1 we deduce that $\mu_1^a \mu_2^a - \mu_3^a \mu_4^a$ is nonzero, so ℓ divides the nonzero integer $N_{F(v)/\mathbb{Q}}(\mu_1^a \mu_2^a - \mu_3^a \mu_4^a)$. By an argument we have used many times we find $\ell \leq (2q_v^a)^{[F(v):\mathbb{Q}]}$, and using the inequality $a < 4(\sqrt{6g} + 1)$ we reach a contradiction. $\square$

11 Proof of theorem 1.2

By corollary 2.4 we see that it is enough to show that G_ℓ contains $\mathrm{Sp}_{2g}(\mathbb{F}_\ell)$, so suppose this is not the case: G_ℓ is then contained in one of the maximal subgroups of $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$ listed in theorem 3.14. Let us go through this list. Given the inequalities imposed on ℓ, proposition 4.1 implies that cases 1 through 3 cannot happen. As for case 4, we have to distinguish according to whether g is even or odd. If g is odd, then case 4 does not arise thanks to proposition 7.5, which can be applied thanks to lemma 7.6. If g is even, then we also need to apply lemma 8.2, and the same conclusion follows. Case 5 is impossible by proposition 10.2.

To exclude case 6 we combine the results of sections 6 and 9. Let H be a maximal subgroup of class $\mathcal{S}$, and suppose by contradiction that G_ℓ is contained in H. Notice first that $\mathbb{P}H$ is almost simple, with socle S of Lie type in characteristic ℓ (proposition 6.8 and lemma 6.9). As we did in section 9, we can then write the finite simple group S as G^F/Z. We let $G, q = \ell^e$ be the associated algebraic data, and consider $A[\ell]$ as the linear representation of G^F corresponding to the projective representation $\mathbb{P}A[\ell]$ of S. Observe next that we have $e = 1$ (proposition 9.38), so we can apply proposition 9.23 to deduce that $A[\ell] \otimes \overline{\mathbb{F}_\ell}$, as a representation of G^F, is isomorphic to $L(\lambda) \cong V(\lambda)$ for some ℓ-restricted weight λ. We now reach a contradiction by applying proposition 9.36.

Suppose lastly that G_ℓ is contained in a maximal subgroup H as in case 7. Using remark 3.16 we see that the order of $\mathbb{P}G_\ell$ does not exceed $J(2g+2)$, and since this contradicts proposition 6.8 we are done.

Finally, it is clear from the explicit expressions of $b([K:\mathbb{Q}], g, h(A))$ that the function $b(g! \cdot [K:\mathbb{Q}], g, h(A))$ grows faster than $b([K:\mathbb{Q}], 2g, 2h(A))^{1/2g}$, and it is easy to check that for $g \geq 19$ the inequality $b(A/K; g!) > b(A^2/K; g)^{1/2g}$ holds for any K and any A. $\square$

12 The tensor product case III – $g = 3$

In this section we show that, when $\dim(A) = 3$, a place v satisfying the hypothesis of proposition 7.5 can be found whose residue characteristic is bounded explicitly in terms of simple arithmetical invariants of A/K. This will be achieved through an application of Chebotarev's theorem, but we shall first need a certain number of preliminaries. We use the notation of §2.3; in particular, if v is a finite place of K we denote by p_v (resp. q_v) the characteristic (resp. the cardinality) of the residue field at v. We also introduce the set

$$\Omega_K^A := \left\{ v \in \Omega_K \;\middle|\; A \text{ has good reduction at } v \text{ and } v \text{ has degree 1 over } \mathbb{Q} \right\}.$$

Most of what we do in this section could be generalized to some extent to other values of g: for example, all results up to corollary 12.11 can easily be extended to cover the case of an arbitrary (odd) *prime* dimension, and it is only the proof of proposition 12.12 that depends on the assumption $\dim A = 3$, since it relies on the particularly simple subgroup structure of $\mathrm{CGO}_3(\mathbb{F}_\ell)$. Trying to generalize this result to other values of $g \geq 5$ introduces additional complications: the group $\mathrm{GL}_2(\mathbb{F}_\ell) \otimes \mathrm{CGO}_g(\mathbb{F}_\ell)$ contains families of maximal proper subgroups of Lie type which we cannot exclude by simply looking at the action of inertia on $A[\ell]$. In section 13 we shall see a way to partially overcome these difficulties, but at present it seems that our methods become more and more cumbersome to apply as the dimension of A increases.

It is also interesting to compare our arguments with those used by Serre [Ser00b] to prove his open image theorem for abelian varieties of odd dimension with $\mathrm{End}_{\overline{K}}(A) = \mathbb{Z}$. It is not hard to realize that a major stumbling block in our approach is the fact that there is no clear analogue of Sen's theorem [Sen73] for representations over $\mathbb{F}_\ell$. Indeed, Serre's approach to prove that G_{ℓ^∞} cannot be contained in an 'exceptional' group of Lie type is based on Sen's theorem, which in turn depends on the completeness of $\mathbb{C}_p$: unfortunately, no modulo-ℓ analogue of this theorem is available, and in fact it is not even clear what such an analogue should look like.

12.1 Decomposition of the eigenvalues of Fr_v

We start with two easy lemmas which do not depend on the assumption $\dim A = 3$:

Lemma 12.1. *Let N be a positive integer no less than 3. Suppose all the torsion points of A of order N are defined over K, and let v be any place of K of good reduction for A and not dividing N. The group generated by the eigenvalues of Fr_v does not contain any nontrivial root of unity.*

Proof. Let $\mu_1, \ldots, \mu_{2g}$ be the eigenvalues of Fr_v. Looking at the action of Fr_v on $A[N]$ we see that each of them (hence every element of the group they generate) is congruent to 1 modulo N, but as it is well known there are no nontrivial roots of unity congruent to 1 modulo N when $N \geq 3$. □

Lemma 12.2. *Let N be a positive integer no less than $2g + 1$. Suppose all the torsion points of A of order N are defined over K, and let v be a place in Ω_K^A. If p_v does not divide N and is larger than $(2g)^2$, then p_v does not divide $\mathrm{tr}\,\mathrm{Fr}_v$.*

Proof. On the one hand $\mathrm{Gal}\left(\overline{K}/K\right)$ acts trivially on $A[N]$, so $\operatorname{tr}\mathrm{Fr}_v$ cannot be zero since it is congruent to $2g$ modulo N. On the other hand, the Weil conjectures imply that $|\operatorname{tr}\mathrm{Fr}_v|$ does not exceed $2g \cdot p_v^{1/2}$, so if p_v divides $|\operatorname{tr}\mathrm{Fr}_v| \neq 0$ we must have $p_v \leq 2g \cdot p_v^{1/2}$, which is equivalent to $p_v \leq (2g)^2$. $\square$

We now specialize to the case $\dim A = 3$. Notice that all tensor product subgroups of $\mathrm{GSp}_6(\mathbb{F}_\ell)$ are of type $(1,3)$, that is, up to conjugation they can be identified with the group $\mathrm{GL}_2(\mathbb{F}_\ell)\otimes\mathrm{CGO}_3(\mathbb{F}_\ell)$. The following proposition imposes stringent restrictions on a Frobenius whose eigenvalues define a point of $U_{13}(\overline{\mathbb{Q}})$:

Proposition 12.3. *Let A/K be an abelian variety of dimension 3 and N be an integer no less than $2g+1=7$. Suppose all the torsion points of A of order N are defined over K and let v be a place of K that satisfies:*

- *$v \in \Omega_K^A$ and $p_v > \max\left\{N, (2g)^2\right\}$;*
- *the eigenvalues $(\mu_1,\ldots,\mu_6)$ of Fr_v define a point of $\bigcup_{\sigma\in S_6} U_{13}^\sigma(\overline{\mathbb{Q}})$, i.e. Fr_v does not satisfy the hypothesis of proposition 7.5.*

Then at least one of the following holds:

1. *there exist algebraic integers λ_1,λ_2 such that the eigenvalues of Fr_v are given by λ_1 and λ_2, both with multiplicity $g=3$;*
2. *for any choice of $\lambda_1,\lambda_2,\beta$ of $\overline{\mathbb{Q}}^\times$ such that the multisets $\left\{\lambda_i\beta, \lambda_i, \lambda_i\beta^{-1} \mid i=1,2\right\}$ and $\{\mu_1,\ldots,\mu_6\}$ coincide, the algebraic number $\lambda_1+\lambda_2$ is not an integer (at least one valid choice of λ_i,β exists by lemma 7.4).*

Proof. Notice first that, by lemma 12.2, the residue characteristic p_v does not divide the (nonzero) integer $\operatorname{tr}\mathrm{Fr}_v$. Let now λ_1,λ_2 and β be algebraic numbers such that the eigenvalues of Fr_v are λ_1,λ_2 and $\lambda_i\beta^{\pm1}$ for $i=1,2$. As the eigenvalues of Fr_v are algebraic integers, this implies in particular that λ_1,λ_2 are algebraic integers. If $\lambda_1+\lambda_2$ is not an integer for any choice of λ_i,β we are done, hence (without loss of generality) we can work under the additional assumption that $\lambda_1+\lambda_2$ is an integer. We are thus reduced to showing that $\beta=1$: this we shall do by proving that β is a root of unity, and then applying lemma 12.1. Let w be any place of $\overline{\mathbb{Q}}$. Suppose first that the residual characteristic of w is not p_v: the Weil conjectures imply that the eigenvalues of Fr_v are units away from p_v, hence $\operatorname{ord}_w(\lambda_i\beta)=\operatorname{ord}_w(\lambda_i\beta^{-1})=0$, which immediately gives $\operatorname{ord}_w(\beta)=0$.

Suppose now that the residual characteristic of w is p_v. As $\operatorname{tr}\mathrm{Fr}_v\neq 0$ can also be written as $(\lambda_1+\lambda_2)\left(1+\beta+\beta^{-1}\right)$ we see that $\lambda_1+\lambda_2$ is nonzero. If $\operatorname{ord}_w(\lambda_i)$ is positive for $i=1,2$, then $\operatorname{ord}_w(\lambda_1+\lambda_2)$ is positive as well and therefore (since $\lambda_1+\lambda_2$ is an integer) we see that p_v divides $\lambda_1+\lambda_2$. However, the Weil conjectures also imply that $|\lambda_1+\lambda_2|\leq 2\sqrt{p_v}$, which – combined with the fact that $\lambda_1+\lambda_2$ is nonzero – gives a contradiction for $p_v\geq 5$ (and our assumptions entail in particular $p_v>(2g)^2=36$), so without loss of generality we can assume $\operatorname{ord}_w(\lambda_1)=0$. Now since $\lambda_1\beta$ and $\lambda_1\beta^{-1}$ are algebraic integers they both have non-negative valuation at w, so we have

$$0\leq\operatorname{ord}_w(\lambda_1\beta)=\operatorname{ord}_w(\beta),\quad 0\leq\operatorname{ord}_w(\lambda_1\beta^{-1})=-\operatorname{ord}_w(\beta),$$

and therefore $\operatorname{ord}_w(\beta)=0$. It follows that the algebraic number β has zero valuation at all places of $\overline{\mathbb{Q}}$ and is therefore a root of unity; by lemma 12.1, this implies $\beta=1$. $\square$

We now proceed to give a sufficient criterion for case (2) of the previous proposition not to happen. The criterion is not new, and can be deduced for example from [Chi92, Sublemmas 5.2.3 and 5.2.4]; however, given that our setting is slightly different and the statement itself differs from Chi's, we reproduce the argument in full for the reader's convenience. Before discussing this criterion we set up some notation.

Definition 12.4. We say that a Frobenius element Fr_v is **of tensor product type** if the multiset Δ of eigenvalues of Fr_v can be written as

$$\Delta = \left\{ \lambda_i, \lambda_i \beta^{\pm 1} \mid i = 1, 2 \right\}$$

for some choice of λ_i, β in $\overline{\mathbb{Q}}^{\times}$. When this is the case, we write Ψ (resp. Λ) for the multiset $\left\{1, \beta^{\pm 1}\right\}$ (resp. $\{\lambda_1, \lambda_2\}$), and we also write symbolically $\Delta = \Lambda \cdot \Psi$.

Remark 12.5. *A priori*, the eigenvalues of Fr_v could admit more than one decomposition as in the previous definition. We shall be careful to distinguish those statements that hold for *any* such decomposition from those that hold for a *fixed* decomposition. Also notice that lemma 7.4 amounts to saying that a Frobenius Fr_v is of tensor product type if and only if its eigenvalues define a point of $\bigcup_{\sigma \in S_6} U_{13}^{\sigma}(\overline{\mathbb{Q}})$.

We now introduce a weak notion of multiplicative independence for the eigenvalues of a Frobenius Fr_v of tensor product type. Fix sets Λ and Ψ as in definition 12.4, and consider the equation

$$(x_1\psi_1)^2 = (x_2\psi_2)(x_3\psi_3) \tag{8}$$

in unknowns $x_1, x_2, x_3 \in \Lambda$ and $\psi_1, \psi_2, \psi_3 \in \Psi$. Notice that this equation admits two obvious families of solutions: if we take $x_1 = x_2 = x_3$, the equation reduces to $\psi_1^2 = \psi_2\psi_3$, which for all $\psi \in \Psi$ admits the solutions $1^2 = \psi \cdot \psi^{-1}$ and $\psi^2 = \psi \cdot \psi$; if no other solution exists, we say that the eigenvalues of Fr_v are weakly independent. More precisely, we give the following definition:

Definition 12.6. We say that the eigenvalues of Fr_v are **weakly independent** (with respect to a given decomposition of $\Delta = \Lambda \cdot \Psi$) if the following two conditions hold:

1. the eigenvalues of Fr_v are all distinct;
2. if $(x_1, x_2, x_3, \psi_1, \psi_2, \psi_3) \in \Lambda^3 \times \Psi^3$ is a solution to equation (8), then $x_1 = x_2 = x_3$ holds and there exists $\psi \in \Psi$ such that we have either $(\psi_1, \psi_2, \psi_3) = (1, \psi, \psi^{-1})$ or $(\psi_1, \psi_2, \psi_3) = (\psi, \psi, \psi)$.

A first useful feature of the notion of weak independence is that it entails uniqueness of the decomposition $\Delta = \Lambda \cdot \Psi$:

Lemma 12.7. *Suppose that* Fr_v *is of tensor product type and that its eigenvalues are weakly independent with respect to a certain decomposition* $\Delta = \Lambda \cdot \Psi$*: then* $\lambda_1 + \lambda_2$ *is an integer, and for any decomposition* $\Delta = \Lambda' \cdot \Psi'$ *of* Δ *we have* $\Lambda' = \Lambda$ *and* $\Psi = \Psi'$.

Proof. We start by describing a property that characterizes λ_1, λ_2 among the elements of Δ. For every $\gamma \in \Delta$ we consider the map

$$\begin{array}{rccc} T_\gamma : & \Delta & \to & \overline{\mathbb{Q}}^{\times} \\ & \delta & \mapsto & \frac{\gamma^2}{\delta}. \end{array}$$

Claim. We have $|T_\gamma(\Delta) \cap \Delta| \geq g = 3$ if and only if γ belongs to Λ.

Proof of claim. The "if" part is trivial: if $\gamma = \lambda_i$, then it is clear that $T_{\lambda_i}(\lambda_i \psi) \in \Delta$ for all $\psi \in \Psi$; as T_γ is injective, this gives $|\Psi| = 3$ elements in the intersection $T_\gamma(\Delta) \cap \Delta$.

Conversely, suppose that $|T_\gamma(\Delta) \cap \Delta| \geq 3$ for a certain $\gamma \in \Delta$. Write $\gamma = x_1 \psi_1$ with $x_1 \in \Lambda, \psi_1 \in \Psi$ and suppose $\psi_1 \neq 1$. Let $x_2 \psi_2 \in \Delta$ be such that $T_\gamma(x_2\psi_2) \in \Delta$. By definition, this implies the existence of $x_3 \in \Lambda, \psi_3 \in \Psi$ that satisfy

$$\frac{(x_1\psi_1)^2}{x_2\psi_2} = x_3\psi_3,$$

and since the eigenvalues are weakly independent we have $x_2 = x_1$ and $\psi_2 = \psi_1$ (since $\psi_1 \neq 1$). Hence we see that $\lambda_1\psi_1$ is the only eigenvalue δ of Fr_v such that $T_\gamma(\delta)$ belongs to Δ, contradicting the fact that $|T_\gamma(\Delta) \cap \Delta| \geq g = 3$.

Notice now that λ_1 and λ_2, being eigenvalues of Fr_v, are algebraic integers, so in order to show that $\lambda_1 + \lambda_2$ is an integer it suffices to prove that it is a rational number, i.e. that the set $\{\lambda_1, \lambda_2\}$ is $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$-invariant. By the previous characterization of λ_1, λ_2 it then suffices to show that for every $\sigma \in \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$ we have $\left|T_{\sigma(\lambda_i)}(\Delta) \cap \Delta\right| \geq g = 3$, and this follows from

$$\left|T_{\sigma(\lambda_i)}(\Delta) \cap \Delta\right| = \left|T_{\sigma(\lambda_i)}(\sigma(\Delta)) \cap \sigma(\Delta)\right| = |T_{\lambda_i}(\Delta) \cap \Delta| \geq g = 3,$$

where we have used the equality $\sigma(\Delta) = \Delta$ (the set Δ is $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$-stable since the characteristic polynomial of Fr_v has integral coefficients).

Moreover, the characterization we have given of λ_1, λ_2 does not use the decomposition of Δ we have fixed, hence it uniquely determines the values of λ_1, λ_2 in any possible decomposition $\Delta = \Lambda' \cdot \Psi'$. We now show that the set Ψ is uniquely determined as well. Let $\Delta = \Lambda \cdot \Psi'$ be any decomposition of Δ, with $\Psi' = \left\{1, (\beta')^{\pm 1}\right\}$, and suppose that $\beta' \neq \beta^{\pm 1}$. By definition, $\mu = \lambda_1\beta$ is an element of Δ, hence it can be written as $\mu = \lambda_i \psi'$ for some $\psi' \in \Psi'$ and some $i \in \{1, 2\}$. As the eigenvalues of Fr_v are all distinct we necessarily have $\psi' \neq 1$; furthermore, if we had $i = 1$ we would also have $\psi' = \beta$, a contradiction, so (replacing β' by $(\beta')^{-1}$ if necessary) we must in fact have $\mu = \lambda_2\beta'$. It follows that β' is equal to $\frac{\lambda_1}{\lambda_2}\beta$ and hence Δ also contains $\lambda_1\beta' = \frac{\lambda_1^2}{\lambda_2}\beta$, which in turn must be of the form $\lambda_k\psi$ for some $k \in \{1, 2\}$ and $\psi \in \Psi$. Thus we find that $\frac{(\lambda_1\beta)^2}{\lambda_2\beta} = \lambda_k\psi$ is a solution to equation (8), so by definition of weak independence we must have $\lambda_1 = \lambda_2$, which is absurd since the eigenvalues of Fr_v are all distinct. The contradiction shows that $\beta' = \beta$, that is, $\Psi' = \Psi$. □

We also need a version of definition 12.6 for operators acting on $\mathbb{F}_\ell^{2g}$:

Definition 12.8. Let h be an element of $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$. If the multiset Δ_ℓ of eigenvalues of h in $\overline{\mathbb{F}_\ell}^\times$ can be written as $\Lambda_\ell \cdot \Psi_\ell$, where $\Lambda_\ell = \{\lambda_1, \lambda_2\}$ and $\Psi_\ell = \left\{1, \beta^{\pm 1}\right\}$ for some $\lambda_i, \beta \in \overline{\mathbb{F}_\ell}^\times$, we say that h is of tensor product type (modulo ℓ). If furthermore the elements of Δ_ℓ are all distinct, and the equality $(x_1\psi_1)^2 = (x_2\psi_2)(x_3\psi_3)$ with $x_i \in \Lambda_\ell, \psi_j \in \Psi_\ell$ implies $x_1 = x_2 = x_3$ and either $(\psi_1, \psi_2, \psi_3) = (1, \psi, \psi^{-1})$ or $(\psi_1, \psi_2, \psi_3) = (\psi, \psi, \psi)$ for some $\psi \in \Psi_\ell$, then we say that h has weakly independent eigenvalues modulo ℓ.

As the proof of lemma 12.7 does not use any particular features of the field $\mathbb{Q}$, the same argument also shows:

Lemma 12.9. *Suppose $h \in \mathrm{GSp}_{2g}(\mathbb{F}_\ell)$ is of tensor product type and has weakly independent eigenvalues modulo ℓ: then the decomposition $\Delta_\ell = \Psi_\ell \cdot \Lambda_\ell$ is unique.*

Lemma 12.10. *Let v be a place in Ω_K^A. Suppose that Fr_v is of tensor product type and ℓ is a prime different from p_v: then $\rho_\ell(\mathrm{Fr}_v)$ is of tensor product type. If furthermore $\rho_\ell(\mathrm{Fr}_v)$ has weakly independent eigenvalues modulo ℓ (for some, hence for any, decomposition of Δ_ℓ as $\Lambda_\ell \cdot \Psi_\ell$), then Fr_v has weakly independent eigenvalues as well. In particular, the decomposition $\Delta = \Lambda \cdot \Psi$ of the eigenvalues of Fr_v is unique, and it satisfies $\lambda_1 + \lambda_2 \in \mathbb{Z}$.*

Proof. The first statement is clear: a decomposition of the eigenvalues of Fr_v induces an analogous decomposition of the eigenvalues of $\rho_\ell(\mathrm{Fr}_v)$. As for the second part, notice first that by assumption the eigenvalues of $\rho_\ell(\mathrm{Fr}_v)$ are distinct, hence the eigenvalues of Fr_v are a fortiori distinct, and there is a *unique* way to lift an eigenvalue of $\rho_\ell(\mathrm{Fr}_v)$ to an eigenvalue of Fr_v. Denote by Δ (resp. Δ_ℓ) the set of eigenvalues of Fr_v (resp. of $\rho_\ell(\mathrm{Fr}_v)$); by assumption, there exists a decomposition $\Delta = \Lambda \cdot \Psi$, which induces an analogous decomposition $\Delta_\ell = \Lambda_\ell \cdot \Psi_\ell$. The multiset Δ does not contain elements with multiplicity greater than 1, so the map

$$\begin{array}{ccc} \Lambda \times \Psi & \to & \Delta \\ (\lambda, \psi) & \mapsto & \lambda\psi \end{array}$$

is a bijection: equivalently, for every eigenvalue δ of Fr_v, *in the given decomposition* $\Lambda \cdot \Psi$ there exist unique $\lambda \in \Lambda$ and $\psi \in \Psi$ such that $\delta = \lambda \cdot \psi$. Repeating the same argument modulo ℓ we find that $\Psi \times \Lambda \to \Delta \to \Delta_\ell \to \Psi_\ell \times \Lambda_\ell$ is a bijection. Consider now the equation

$$(x_1\psi_1)^2 = (x_2\psi_2)(x_3\psi_3)$$

with $x_i \in \Lambda$ and $\psi_j \in \Psi$. Reducing modulo ℓ and using the weak independence of the eigenvalues of $\rho_\ell(\mathrm{Fr}_v)$ we see that $x_1 = x_2 = x_3$ (as elements of Λ_ℓ), and either $\psi_1 = \psi_2 = \psi_3$ or $\psi_1 = 1$ and $\psi_2 = \psi_3^{-1}$ (as elements of Ψ_ℓ). Using the fact that $\Psi \times \Lambda \to \Psi_\ell \times \Lambda_\ell$ is a bijection we then conclude that we also have $x_1 = x_2 = x_3$ as elements of Λ, and that (ψ_1, ψ_2, ψ_3) is either of the form $(1, \psi, \psi^{-1})$ or of the form (ψ, ψ, ψ) for some $\psi \in \Psi$. The remaining statements follow immediately from lemma 12.7. □

We finally come to the result which will allow us to find Frobenius elements not of tensor product type:

Corollary 12.11. *Let N be an integer no less than $2g + 1 = 7$. Suppose that all the torsion points of A of order N are defined over K, and let $v \in \Omega_K^A$ satisfy $p_v > \max\{N, (2g)^2\}$. Suppose furthermore that for some prime ℓ different from p_v the image $\rho_\ell(\mathrm{Fr}_v)$ is of tensor product type and has weakly independent eigenvalues modulo ℓ. Then Fr_v is **not** of tensor product type.*

Proof. Suppose Fr_v is of tensor product type: then it satisfies the assumptions of lemma 12.10, so in the (unique) decomposition of its eigenvalues as $\Lambda \cdot \Psi$ we must have $\lambda_1 + \lambda_2 \in \mathbb{Z}$. Furthermore, the eigenvalues of Fr_v are all distinct (since this is true when they are regarded modulo ℓ). On the other hand, Fr_v also satisfies the hypotheses of proposition 12.3 (cf. remark 12.5), hence one of the two conclusions of that proposition must hold: but this is absurd by what we just proved, and the contradiction shows the result. □

We now just need to find a Frobenius Fr_v as in the previous corollary: this will be achieved thanks to Chebotarev's theorem, but we first need one more lower bound on G_ℓ (recall that the group $\Omega_3(\mathbb{F}_\ell)$ was introduced in definition 3.8):

Proposition 12.12. *Suppose that the 7-torsion of A is defined over K: then for all primes ℓ unramified in K and strictly larger than $b(A^2/K;3)^{1/6}$ we have $G_\ell \supseteq \mathrm{SL}_2(\mathbb{F}_\ell) \otimes \Omega_3(\mathbb{F}_\ell)$ (up to conjugacy).*

Proof. This is very similar to what we did in the previous sections, so we keep details to a minimum. We first observe that since $A[7]$ is defined over K the abelian variety A has semistable reduction at every place v of K of characteristic $\neq 7$ (this is a theorem of Raynaud, cf. [GRR72, Proposition 4.7]). Notice now that we can assume that (up to conjugation) G_ℓ is contained in $\mathrm{GL}_2(\mathbb{F}_\ell) \otimes \mathrm{CGO}_3(\mathbb{F}_\ell)$, for otherwise the proof of theorem 1.2 shows that G_ℓ contains all of $\mathrm{Sp}_6(\mathbb{F}_\ell)$. Also notice that the group $\mathrm{GL}_2(\mathbb{F}_\ell) \otimes \mathrm{CGO}_3(\mathbb{F}_\ell)$ admits well-defined projections π_2, π_3 to $\mathrm{PGL}_2(\mathbb{F}_\ell)$ and $\mathbb{P}\mathrm{CGO}_3(\mathbb{F}_\ell)$ respectively. Observe now that the tensor product structure implies that if either projection stabilizes a subspace (respectively in $\mathbb{F}_\ell^2$ or in $\mathbb{F}_\ell^3$), then the same is true for all of G_ℓ: indeed, if W is a point of $\mathbb{P}\left(\mathbb{F}_\ell^2\right)$ (i.e. a line in $\mathbb{F}_\ell^2$) stable under the action of $\pi_2(G_\ell)$, then $W \otimes \mathbb{F}_\ell^3$ is a proper subspace of $\mathbb{F}_\ell^6$ stable under the action of G_ℓ, and the same argument applies to π_3 as well. In particular, proposition 4.1 implies that neither projection stabilizes a linear subspace. We now show that the two projections are in fact surjective.

Surjectivity on $\mathbb{P}\Omega_3(\mathbb{F}_\ell) \cong \mathrm{PSL}_2(\mathbb{F}_\ell)$. From [BHRD13, Table 8.7] we see that the maximal subgroups of $\mathbb{P}\mathrm{CGO}_3(\mathbb{F}_\ell)$ that do not contain $\mathbb{P}\Omega_3$ either stabilize a linear subspace or have order at most 120. We have already excluded the first case, and the second case is easily treated as well: replacing K with the extension defined by $\ker\left(\mathrm{Gal}\left(\overline{K}/K\right) \to G_\ell \to \mathbb{P}\mathrm{CGO}_3(\mathbb{F}_\ell)\right)$ we are back to the case of a group stabilizing a linear subspace, hence this case cannot happen for ℓ in our range (since we have in particular $\ell > b_0(A/K;120)$).

Remark 12.13. Notice that although $\mathbb{P}\Omega_3(\mathbb{F}_\ell)$ and $\mathrm{PSL}_2(\mathbb{F}_\ell)$ are isomorphic as abstract groups, the representation structure of their respective natural modules is very different: in particular, the non-split Cartan subgroups are of class $\mathcal{C}_3$ in $\mathrm{PSL}_2(\mathbb{F}_\ell)$ but of class $\mathcal{C}_1$ in $\mathbb{P}\Omega_3(\mathbb{F}_\ell)$.

(Almost) surjectivity on $\mathrm{PSL}_2(\mathbb{F}_\ell)$. We read from [BHRD13, Table 8.1] that the maximal subgroups of $\mathrm{PGL}_2(\mathbb{F}_\ell)$ that do not contain $\mathrm{PSL}_2(\mathbb{F}_\ell)$ and do not stabilize a linear subspace either contain a normal abelian subgroup of index at most 2, or have order at most 120. The second case is excluded by the same argument as in the previous paragraph, so the image H_2 of G_ℓ in $\mathrm{PGL}_2(\mathbb{F}_\ell)$ contains either $\mathrm{PSL}_2(\mathbb{F}_\ell)$ or an abelian subgroup C_2 of index at most 2; furthermore, in the latter case there is no loss of generality in assuming that $|C_2| > 60$ (for otherwise H_2 has order at most 120, which we have already excluded).

Surjectivity on both factors. Let $H_2 = \pi_2(G_\ell), H_3 = \pi_3(G_\ell)$. We consider the image of G_ℓ in $\mathrm{PGL}_2(\mathbb{F}_\ell) \times \mathbb{P}\mathrm{CGO}_3(\mathbb{F}_\ell)$: it is a subgroup H of $H_2 \times H_3$ that projects surjectively on the factors H_2, H_3. We also know that H_3 contains $\mathbb{P}\Omega_3(\mathbb{F}_\ell)$. Suppose by contradiction that H_2 contains an abelian subgroup C_2 of index at most 2 and replace K with its (at most) quadratic extension K' defined by $\ker\left(\mathrm{Gal}\left(\overline{K}/K\right) \to G_\ell \to H_2 \to H_2/C_2\right)$. This has the effect of replacing H_2 with C_2; at the same time H_3 gets replaced by a subgroup C_3 of index at most 2, and since $\mathbb{P}\Omega_3(\mathbb{F}_\ell)$ does not have subgroups of index 2 we see that $C_3 \supseteq \mathbb{P}\Omega_3(\mathbb{F}_\ell)$. Finally, G_ℓ is replaced by a subgroup $\tilde{G}_\ell$ of index at most 2, and likewise H gets replaced by a subgroup C of index at most 2, which satisfies $C \subseteq C_2 \times C_3$ and projects surjectively on both C_2 and C_3. Let now $N_3 := \ker(C \to C_2)$ and $N_2 := \ker(C \to C_3)$, considered as subgroups of C_3, C_2 respectively. By Goursat's lemma we know that the quotients C_3/N_3 and C_2/N_2 are isomorphic, and in particular abelian (as C_2 is). Since the group $\mathbb{P}\mathrm{CGO}_3(\mathbb{F}_\ell)$ is almost

simple with socle $\mathbb{P}\Omega_3(\mathbb{F}_\ell)$, it is clear that N_3 contains all of $\mathbb{P}\Omega_3(\mathbb{F}_\ell)$, so the quotient C_3/N_3 has order at most 2. Hence N_2 has in turn index at most 2 in C_2, and therefore there is a nontrivial element α in N_2 (recall that $|C_2| > 60$). By definition of N_2, this α projects to the identity in C_3, so any element $\tilde{\alpha} \in \tilde{G_\ell}$ lifting α is central in $\tilde{G_\ell}$. In particular, the centralizer of $\tilde{G_\ell}$ in $\operatorname{Aut} A[\ell]$ is larger than $\mathbb{F}_\ell$, and by proposition 4.1 this is a contradiction for ℓ larger than $b(A^2/K')^{1/6}$, a quantity which is smaller than $b(A^2/K;3)^{1/6}$. The contradiction shows the result.

G_ℓ **contains** $\mathrm{SL}_2(\mathbb{F}_\ell)\otimes\Omega_3(\mathbb{F}_\ell)$**.** Notice that it is enough to show that H (the image of $\pi_2\times\pi_3$) contains $\mathrm{PSL}_2(\mathbb{F}_\ell)\times\mathbb{P}\Omega_3(\mathbb{F}_\ell)$. Indeed, if this is the case, then for every $\overline{x_2}\in\mathrm{PSL}_2(\mathbb{F}_\ell)$ we can find an $x\in G_\ell$ with $\pi_2(x)=\overline{x_2}$ and $\pi_3(x)=\mathrm{Id}$, that is G_ℓ contains a certain x that can be written as $x=x_2\otimes\mathrm{Id}$ for some $x_2\in\mathrm{GL}_2(\mathbb{F}_\ell)$ lifting $\overline{x_2}$. Consider now the subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$ given by $\left\{x\in\mathrm{GL}_2(\mathbb{F}_\ell)\;\middle|\;x\otimes\mathrm{Id}\in G_\ell\right\}$: by what we just said, this group projects surjectively onto $\mathrm{PSL}_2(\mathbb{F}_\ell)$, hence it contains all of $\mathrm{SL}_2(\mathbb{F}_\ell)$. It follows that G_ℓ contains $\mathrm{SL}_2(\mathbb{F}_\ell)\otimes\{\mathrm{Id}\}$, and by the same argument applied to π_3 we also have $\{\mathrm{Id}\}\otimes\Omega_3(\mathbb{F}_\ell)\subseteq G_\ell$, which implies that G_ℓ contains $\mathrm{SL}_2(\mathbb{F}_\ell)\otimes\Omega_3(\mathbb{F}_\ell)$ as claimed.

So let again $H_2=\pi_2(G_\ell)$ and $H_3=\pi_3(G_\ell)$, where we now know that H_2 (resp. H_3) contains $\mathrm{PSL}_2(\mathbb{F}_\ell)$ (resp. $\mathbb{P}\Omega_3(\mathbb{F}_\ell)$). Let N_2,N_3 be the kernels of $H\to H_3$, $H\to H_2$ respectively, considered as subgroups of H_2,H_3, and recall that by Goursat's lemma the image of H in $H_2/N_2\times H_3/N_3$ is the graph of an isomorphism $H_2/N_2\xrightarrow{\sim}H_3/N_3$. Now N_2 is a normal subgroup of H_2, so either it contains all of $\mathrm{PSL}_2(\mathbb{F}_\ell)$ or it is trivial: in the former case we have $|H_3/N_3|=|H_2/N_2|\le 2$, which clearly implies that N_3 contains $\mathbb{P}\Omega_3(\mathbb{F}_\ell)$ and H contains $N_2\times N_3\supseteq\mathrm{PSL}_2(\mathbb{F}_\ell)\times\mathbb{P}\Omega_3(\mathbb{F}_\ell)$ as claimed. On the other hand, if N_2 is the trivial group then H is the graph of an isomorphism $H_2\to H_3$; up to conjugation, such an isomorphism is necessarily the 3-dimensional orthogonal projective representation of either $\mathrm{PGL}_2(\mathbb{F}_\ell)$ or $\mathrm{PSL}_2(\mathbb{F}_\ell)$, according to whether H_2 is $\mathrm{PGL}_2(\mathbb{F}_\ell)$ or $\mathrm{PSL}_2(\mathbb{F}_\ell)$. For simplicity of exposition suppose that $H_2=\mathrm{PSL}_2(\mathbb{F}_\ell)$; the argument is perfectly analogous if $H_2=\mathrm{PGL}_2(\mathbb{F}_\ell)$. Let σ_2 be the second symmetric power of the standard representation of $\mathrm{SL}_2(\mathbb{F}_\ell)$ (which is also the unique 3-dimensional orthogonal representation of $\mathrm{SL}_2(\mathbb{F}_\ell)$), and recall that if $x\in\mathrm{SL}_2(\mathbb{F}_\ell)$ has eigenvalues λ_1,λ_2, then $\sigma_2(x)$ has eigenvalues $\lambda_1^2,\lambda_1\lambda_2,\lambda_2^2$. Now since $\sigma_2(-\mathrm{Id})$ is trivial σ_2 fits into a diagram

$$\begin{tikzcd}
\mathrm{SL}_2(\mathbb{F}_\ell) \arrow[r, "\sigma_2"] \arrow[d, "\pi"'] & \mathrm{CGO}_3(\mathbb{F}_\ell) \arrow[d, "\pi"] \\
\mathrm{PSL}_2(\mathbb{F}_\ell) \arrow[r, dashed, "\mathbb{P}\sigma_2"'] & \mathbb{P}\mathrm{CGO}_3(\mathbb{F}_\ell),
\end{tikzcd}$$

and we have just seen that all $h\in H\subseteq H_2\times H_3$ can be written as $(\pi(x),\mathbb{P}\sigma_2(\pi(x)))$ for some $x\in\mathrm{SL}_2(\mathbb{F}_\ell)$; furthermore, the commutativity of the diagram gives $h=(\pi(x),\pi(\sigma_2(x)))$. Now let $g_2\otimes g_3$ be an element of G_ℓ (with $g_2\in\mathrm{GL}_2(\mathbb{F}_\ell),g_3\in\mathrm{CGO}_3(\mathbb{F}_\ell)$), mapping in H to a certain $h=(\pi(x),\pi(\sigma_2(x)))$: by definition of H, this implies that there are scalars $\nu_2,\nu_3\in\mathbb{F}_\ell^\times$ such that $g_2=\nu_2x$ and $g_3=\nu_3\sigma_2(x)$. If we denote by λ_1,λ_2 the eigenvalues of x we thus see that the eigenvalues of $g_2\otimes g_3$ are given by the pairwise products of $\{\nu_2\lambda_1,\nu_2\lambda_2\}$ and $\{\nu_3\lambda_1^2,\nu_3\lambda_1\lambda_2,\nu_3\lambda_2^2\}$; finally letting $\mu=\nu_2\nu_3$, we have proved that the eigenvalues of any $g_2\otimes g_3\in G_\ell$ can be written as

$$\{\mu\lambda_1,\mu\lambda_2\}\cdot\left\{\lambda_1^2,\lambda_1\lambda_2,\lambda_2^2\right\}=\left\{\mu\lambda_1^3,\mu\lambda_1^2\lambda_2,\mu\lambda_1\lambda_2^2,\mu\lambda_1^2\lambda_2,\mu\lambda_1\lambda_2^2,\mu\lambda_2^3\right\} \tag{9}$$

for some $\mu \in \mathbb{F}_\ell^\times$ and $\lambda_1, \lambda_2 \in \mathbb{F}_{\ell^2}^\times$. It is clear that the we arrive at the same conclusion also if $H_2 = \mathrm{PGL}_2(\mathbb{F}_\ell)$. To conclude the proof we just need to show that the decomposition of eigenvalues given by (9) leads to a contradiction for ℓ large enough, and this can easily be done by the arguments of section 5. We give some detail.

Recall that A has semistable reduction at all places of K of characteristic different from 7. In particular, if we let $\mathfrak{l}$ be any place of K of characteristic ℓ, then A has either good or bad semistable reduction at $\mathfrak{l}$, so we can apply theorem 5.2. Let $W_1, \ldots, W_k$ be the simple Jordan-Hölder quotients of $A[\ell]$ under the action of $I_\mathfrak{l}$ (or equivalently, of $I_\mathfrak{l}^t$). The same argument as in lemma 5.6 implies that every W_i is of dimension at most 2; let m_0 (resp. m_1, m_2) denote the number of simple Jordan-Holder quotients with trivial action of $I_\mathfrak{l}^t$ (resp. with action given by χ_ℓ, by a fundamental character of level 2). Equation (3) and lemma 5.7 still hold in our present context, and a slight variant of lemma 5.8 shows that $m_0 = 0$ for every $\ell \geq 5$ unramified in K; thus we want to exclude the case $m_2 = 3$. As in the proof of lemma 5.9, one sees that the assumption $m_2 = 3$ implies $\lambda_1 = \pm\lambda_2$; on the other hand, for any given $x \in I_\mathfrak{l}^t$ there is a fundamental character of level 2, call it φ, such that $\mu\lambda_1^3 = \varphi(x)$. Since $\chi_\ell(x)^3 = \det \rho_\ell(x) = \mu^6(\lambda_1\lambda_2)^9$ we conclude that for all $x \in I_\mathfrak{l}^t$ we have

$$\chi_\ell(x)^6 = \mu^{12}(\lambda_1\lambda_2)^{18} = \varphi(x)^{12}(\lambda_2/\lambda_1)^{18} = \varphi(x)^{12},$$

whence for all $x \in I_\mathfrak{l}^t$ there is a fundamental character φ of level 2 such that $\varphi^{6(\ell+1)-12}(x) = 1$. As $|\varphi(I_\mathfrak{l}^t)| = \ell^2 - 1$ for both fundamental characters of level 2 this is absurd for $\ell > 7$. □

Finally, a simple combinatorial argument shows:

Lemma 12.14. *For $\ell > 101$ the groups $\mathrm{Sp}_6(\mathbb{F}_\ell)$ and $\mathrm{SL}_2(\mathbb{F}_\ell) \otimes \Omega_3(\mathbb{F}_\ell)$ contain elements of tensor product type with weakly independent eigenvalues (modulo ℓ).*

There are certainly many ways to prove this easy fact, but for the sake of completeness we include a detailed proof:

Proof. Fix a square root $i \in \mathbb{F}_{\ell^2}$ of -1 and an element $a \in \mathbb{F}_\ell^\times$ of multiplicative order at least 5. Let Γ be the multiplicative group $\{c + di \mid (c, d) \in \mathbb{F}_\ell^2,\ c^2 + d^2 = 1\}$, which is isomorphic to either $\mathbb{F}_\ell^\times$ or $\ker\left(\mathrm{Norm} : \mathbb{F}_{\ell^2}^\times \to \mathbb{F}_\ell^\times\right)$ according to whether or not -1 is a square modulo ℓ. Notice that if γ is an element of Γ, then the pair (c, d) is uniquely determined by the equations $c + di = \gamma,\ c - di = 1/\gamma$. We can then consider the injective group morphism

$$\begin{array}{rccc} \sigma : & \Gamma & \to & \mathrm{SL}_2(\mathbb{F}_\ell) \otimes \mathrm{SO}_3(\mathbb{F}_\ell) \\ & \gamma = c + di & \mapsto & \sigma_\gamma := \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \otimes \begin{pmatrix} c & d & 0 \\ -d & c & 0 \\ 0 & 0 & 1 \end{pmatrix}, \end{array}$$

which, since $\mathrm{SL}_2(\mathbb{F}_\ell) \otimes \Omega_3(\mathbb{F}_\ell)$ has index 2 in $\mathrm{SL}_2(\mathbb{F}_\ell) \otimes \mathrm{SO}_3(\mathbb{F}_\ell)$, maps 2Γ into $\mathrm{SL}_2(\mathbb{F}_\ell) \otimes \Omega_3(\mathbb{F}_\ell)$. Since $|\sigma(2\Gamma)| = |2\Gamma| \geq \frac{\ell-1}{2}$, the lemma will follow if we show that the image of σ contains no more than $50 < \frac{\ell-1}{2}$ operators whose eigenvalues are not weakly independent.

It is clear by construction that the eigenvalues of σ_γ are given by the pairwise products of $\Lambda = \{a^{\pm 1}\}$ and $\Psi = \{1, \gamma^{\pm 1}\}$, so σ_γ has weakly independent eigenvalues if and only if all the solutions to the equation $\left(a^{\varepsilon_1}\gamma^{\delta_1}\right)^2 = a^{\varepsilon_2}\gamma^{\delta_2} \cdot a^{\varepsilon_3}\gamma^{\delta_3}$ with $\varepsilon_j \in \{\pm 1\}, \delta_j \in \{0, \pm 1\}$ are given by $\varepsilon_1 = \varepsilon_2 = \varepsilon_3$ and either $\delta_1 = \delta_2 = \delta_3$ or $\delta_1 = 0$ and $\delta_2 = -\delta_3$. Equivalently, σ_γ has weakly independent eigenvalues if and only if the equation $a^m = \gamma^n$ with $m \in \{0, \pm 2, \pm 4\}$ and

$n \in \{0, 1, 2, 3, 4\}$ has only the trivial solution $m = n = 0$. Notice that (independently of γ) there are no nontrivial solutions with $n = 0$, because $|m|$ is at most 4 while a has order at least 5. On the other hand, for fixed a, for each pair $(m, n) \in \{0, \pm 2, \pm 4\} \times \{1, \dots, 4\}$ the equation $a^m = \beta^n$ has at most n solutions β, so in total there are at most $5 \times (1 + 2 + 3 + 4) = 50$ triplets (β, m, n) of solutions to the equation $a^m = \beta^n$. In particular, if γ is different from any of these (at most 50) β, then σ_γ has weakly independent eigenvalues, and by what we already remarked this finishes the proof. $\square$

12.2 Applying Chebotarev's theorem

For the proof of theorem 1.6 we need one last ingredient, namely an effective version of the Chebotarev density theorem. Lagarias and Odlyzko proved such a result in [LO77], but their estimate involved a non-explicit constant (which was however effectively computable in principle); their bound was subsequently improved by Œsterlé, who also computed the constant (cf. [Œ79] and [Ser81, §2.5]). To state Œsterlé's result we fix some notation. We let as usual K be a number field, and denote by Δ_K its absolute discriminant; we also write S for a finite subset of Ω_K (the set of finite places of K). To simplify the formulas that follow it is also useful to introduce the function

$$\Delta^*(K, S, N) := |\Delta_K|^N \left(N \cdot \prod_{v \in S} p_v^{1-1/N} \right)^{N \cdot [K:\mathbb{Q}]},$$

where N is a positive integer, and express the bounds we obtain in terms of the quantity

$$B(K, S, N) = 70 \cdot (\log \Delta^*(K, S, N))^2.$$

Theorem 12.15. *(Effective Chebotarev under GRH, [Œ79]) Assume the Generalized Riemann Hypothesis. Let L/K be a Galois extension of number fields of degree at most N and let S be a set of finite places of K containing the ones the ramify in L. For every conjugacy class C of $\operatorname{Gal}(L/K)$ there is a place v of K satisfying:*

1. *v is of degree 1 over $\mathbb{Q}$ and does not belong to S;*
2. *the image of Fr_v in $\operatorname{Gal}(L/K)$ lies in C;*
3. *$p_v \leq B(K, S, N)$.*

Remark 12.16. Lagarias and Odlyzko also proved a version of theorem 12.15 which does not depend on the Generalized Riemann Hypothesis: more precisely, they showed that the same conclusion holds at the cost of replacing $B(K, S, N)$ by $\Delta^*(K, S, N)^c$, where c is an absolute and effectively computable constant. Unpublished work of Winckler [Win] shows that (for $N \geq 2$) one can take $c = 27175010$, cf. also [Zam15].

We can finally prove theorem 1.6, whose statement we reproduce here for the reader's convenience:

Theorem 12.17. *(Theorem 1.6) Let A/K be an abelian variety of dimension 3 such that $\operatorname{End}_{\overline{K}}(A) = \mathbb{Z}$. Denote by $\mathcal{N}^0_{A/K}$ the naive conductor of A/K, that is, the product of the prime ideals of $\mathcal{O}_K$ at which A has bad reduction, and suppose that $A[7]$ is defined over K.*

- *Assume the Generalized Riemann Hypothesis: then the equality* $G_{\ell^\infty} = \mathrm{GSp}_6(\mathbb{Z}_\ell)$ *holds for every prime* ℓ *unramified in* K *and strictly larger than* $(2q)^{48}$*, where*

$$q = b(A^2/K;3)^8 \left(\log|\Delta_{K/\mathbb{Q}}| + \log N_{K/\mathbb{Q}}\left(\mathcal{N}^0_{A/K}\right)\right)^2.$$

- *Unconditionally, the same conclusion holds with*

$$q = \exp\left(cb(A^2/K;3)^8 \left(\log|\Delta_K| + \log N_{K/\mathbb{Q}}\left(\mathcal{N}^0_{A/K}\right)\right)^2\right),$$

where c *is an absolute, effectively computable constant.*

Proof. Let ℓ_0 be the smallest prime larger than $b(A^2/K;3)^{1/6}$; by Bertrand's postulate we have $\ell_0 \leq 2b(A^2/K;3)^{1/6}$. Let L denote the field $K(A[\ell_0])$. By construction the Galois group $\mathrm{Gal}(L/K)$ is just G_{ℓ_0}, and by proposition 12.12 we know that G_{ℓ_0} contains $\mathrm{SL}_2(\mathbb{F}_\ell)\otimes\Omega_3(\mathbb{F}_\ell)$ and hence, by lemma 12.14, an operator of tensor product type with weakly independent eigenvalues. Let C be the conjugacy class of this operator and set

$$S = \left\{v \in \Omega_K \;\middle|\; p_v \leq (2g)^2 = 36 \text{ or } A \text{ has bad reduction at } v\right\} \cup \left\{v \in \Omega_K \;\middle|\; p_v = \ell_0\right\}$$

and $N = [L:K]$. Clearly $N \leq |\mathrm{GSp}_6(\mathbb{F}_{\ell_0})| < \ell_0^{22} \leq 2^{22} b(A^2/K;3)^{11/3}$ and

$$\begin{aligned}
\log\left(\prod_{v\in S} p_v\right) &\leq \log\left(\ell_0^{[K:\mathbb{Q}]}\cdot\prod_{p<37} p^{[K:\mathbb{Q}]}\cdot\prod_{v \text{ of bad reduction}} p_v\right)\\
&\leq \log N_{K/\mathbb{Q}}(\mathcal{N}^0_{A/K}) + [K:\mathbb{Q}]\,(26.1+\log\ell_0)\\
&< \log N_{K/\mathbb{Q}}(\mathcal{N}^0_{A/K}) + \frac{1}{3}[K:\mathbb{Q}]\log b(A^2/K;3).
\end{aligned}$$

We obtain a (rough) bound on $\Delta^*(K,S,N)$ of the form

$$\begin{aligned}
\log\Delta^*(K,S,N) &\leq N\,\Big(\log|\Delta_K| + [K:\mathbb{Q}]\log N + \\
&\qquad +[K:\mathbb{Q}](\log N_{K/\mathbb{Q}}(\mathcal{N}^0_{A/K}) + \frac{1}{3}[K:\mathbb{Q}]\log b(A^2/K;3))\Big)\\
&\leq \frac{1}{\sqrt{70}} b(A^2/K;3)^4\left(\log|\Delta_K| + \log N_{K/\mathbb{Q}}\left(\mathcal{N}^0_{A/K}\right)\right),
\end{aligned}$$

where on the last line we have used the fact (a deep theorem of Fontaine and Abrashkin) that there are no abelian varieties over $\mathbb{Q}$ having good reduction everywhere, and therefore the term $\log|\Delta_K| + \log N_{K/\mathbb{Q}}\left(\mathcal{N}^0_{A/K}\right)$ is always at least $\log 2$. We now see from theorem 12.15 that there exists a place v of K of degree one, satisfying $v \notin S$,

$$p_v \leq 70\,(\log\Delta^*(K,S,N))^2 = q,$$

and such that Fr_v maps to the conjugacy class C in $\mathrm{Gal}(L/K) = G_{\ell_0}$. By construction of S, we have $p_v > (2g)^2$ and $p_v \neq \ell_0$, and furthermore A has good reduction at v. By corollary 12.11, Fr_v is not of tensor product type.

We now start copying the proof of theorem 1.2. Again we have to go through the list of theorem 3.14. Cases 1, 2 and 3 are treated as in the proof of theorem 1.2 (notice that $(2q)^{48}$

is much larger than either $b(A^2/K;3)^{1/6}$ or $b(A/K;3)$). Cases 5 and 7 do not arise, because $2g=6$ is not a perfect power. Now recall that, as already remarked, A/K has semistable reduction at all places of characteristic ℓ. By corollary 6.6 and proposition 6.4 we know that if G_ℓ is contained in a maximal subgroup H of class $\mathcal{S}$, then $\operatorname{soc}(\mathbb{P}H)$ is of Lie type in characteristic ℓ. By [BHRD13, Table 8.29] we see that in fact we have $\operatorname{soc}(\mathbb{P}H) \cong \mathrm{PSL}_2(\mathbb{F}_\ell)$, but this cannot happen (in our range of ℓ) because of proposition 5.10. This excludes case 6. Finally, to see that case 4 cannot arise we simply apply proposition 7.5 to the place v we constructed above.

If we do not assume the Generalized Riemann Hypothesis, we get the desired conclusion by applying the unconditional version of the effective Chebotarev theorem, cf. remark 12.16. ☐

Remark 12.18. The assumption that $A[7]$ is defined over K is not a serious restriction. Let A/K_0 be any abelian threefold with absolutely trivial endomorphism ring and let K be the field $K_0(A[7])$. Clearly if for some prime ℓ the representation $\rho_\ell^{(K)} : \operatorname{Gal}\left(\overline{K}/K\right) \to \operatorname{GSp}(A[\ell])$ is surjective, then the same is true for the representation $\rho_\ell^{(K_0)} : \operatorname{Gal}\left(\overline{K_0}/K_0\right) \to \operatorname{GSp}(A[\ell])$, so it suffices to give an effective bound ℓ_0 such that $\rho_\ell^{(K)}$ is surjective for $\ell > \ell_0$. Let $S_0 \subseteq \Omega_{K_0}$ be the set of places of bad reduction of A. The extension K/K_0 has degree bounded by $N := |\operatorname{GL}_6(\mathbb{F}_7)|$, and it ramifies at most at the places of S_0 and at those of characteristic 7; set $S = S_0 \cup \left\{ v \in \Omega_{K_0} \;\middle|\; p_v = 7 \right\}$. It follows from [Ser81, Proposition 5] that

$$|\Delta_K| \leq \Delta^*(K_0, S, N) < \Delta_{K_0}^N \cdot \left(7^{[K:\mathbb{Q}]} N\right)^{N[K:\mathbb{Q}]} \cdot \left(N_{K_0/\mathbb{Q}} \mathcal{N}^0_{A/K_0}\right)^{N[K:\mathbb{Q}]},$$

and we can then apply theorem 12.17 to A/K to get an effective bound ℓ_0 as above.

13 An effective bound in dimension 5

In this paragraph we show that the methods developed in the previous sections can be pushed further, and for some values of the dimension g they yield an effective bound $\ell_0(A/K)$ such that $G_\ell = \operatorname{GSp}_{2g}(\mathbb{F}_\ell)$ for all $\ell > \ell_0(A/K)$. The method outlined here can be made to work in greater generality, but for simplicity of exposition (and since the precise assumptions needed on $\dim A$ are cumbersome to state) we stick to the relatively simple case $\dim A = 5$. In particular, we let A/K be a 5-dimensional abelian variety with $\operatorname{End}_{\overline{K}}(A) = \mathbb{Z}$ such that $A[2g+1] = A[11]$ is defined over K. We aim to show the following:

Proposition 13.1. *There is an effective bound $\ell_0(A/K)$ (depending on $h(A)$, on the discriminant Δ_K of K, and on $\mathcal{N}^0_{A/K}$) such that $G_\ell = \operatorname{GSp}_{10}(\mathbb{F}_\ell)$ for every $\ell > \ell_0(A/K)$.*

We start with the following simple lemma in algebraic number theory:

Lemma 13.2. *Let p be a prime number and $\lambda_1, \lambda_2, \lambda_3$ be algebraic integers of degree 2 over $\mathbb{Q}$ that are p-Weil numbers of weight 1 (that is, $|\lambda_i| = p^{1/2}$ under any embedding of $\overline{\mathbb{Q}}$ in $\mathbb{C}$). Suppose that:*

- $\operatorname{tr}\lambda_1, \operatorname{tr}\lambda_2$ *and* $\operatorname{tr}\lambda_3$ *do not vanish;*
- *the multiplicative subgroup of $\overline{\mathbb{Q}}^\times$ generated by $\lambda_1, \lambda_2, \lambda_3$ is torsion-free.*

The equality $\lambda_2^2 = \lambda_1\lambda_3$ implies $\lambda_1 = \lambda_2 = \lambda_3$.

Proof. Notice first that $\lambda_1, \lambda_2, \lambda_3$ are not real numbers: indeed, the only real p-Weil numbers of weight 1 are $\pm\sqrt{p}$, which have zero trace. For $i = 1, \dots, 3$ fix now a squarefree integer d_i such that $\mathbb{Q}(\lambda_i) = \mathbb{Q}(\sqrt{d_i})$; by what we have just observed, every d_i is negative.

- Case 1: $\mathbb{Q}(\lambda_1) = \mathbb{Q}(\lambda_3)$. Write for simplicity $F = \mathbb{Q}(\lambda_1) = \mathbb{Q}(\lambda_3)$: it is a quadratic imaginary field. Notice first that $\lambda_1\lambda_3$ cannot be a rational number, for otherwise the trace of $\lambda_2 = \pm\sqrt{\lambda_1\lambda_3}$ would be zero; since $[\mathbb{Q}(\lambda_2) : \mathbb{Q}] = 2$, it follows that $\lambda_1\lambda_3$ is a square in F and therefore λ_2 belongs to F.

  Since λ_i (for $i = 1, 2, 3$) has norm p by assumption, we see that the principal ideals (λ_i) of $\mathcal{O}_F$ are prime. It follows from the equation $\lambda_2^2 = \lambda_1\lambda_3$ and unique factorization in ideals that we have the equality $(\lambda_1) = (\lambda_2) = (\lambda_3)$ of principal ideals. As F is an imaginary quadratic field, the only units of $\mathcal{O}_F$ are the roots of unity in F, hence we have $\lambda_2 = \mu_1\lambda_1 = \mu_3\lambda_3$ for some roots of unity μ_1, μ_3. The assumption that the subgroup of $\overline{\mathbb{Q}}^\times$ generated by $\lambda_1, \lambda_2, \lambda_3$ is torsion-free now implies $\mu_1 = \mu_3 = 1$.

- Case 2: $\mathbb{Q}(\lambda_1) \neq \mathbb{Q}(\lambda_3)$. This implies that $F := \mathbb{Q}\left(\sqrt{d_1}, \sqrt{d_3}\right)$ is a degree-4 extension of $\mathbb{Q}$ with Galois group $(\mathbb{Z}/2\mathbb{Z})^2$. A basis of F over $\mathbb{Q}$ is given by $1, \sqrt{d_1}, \sqrt{d_3}, \sqrt{d_1d_3}$. Write $\lambda_i = a_i + b_i\sqrt{d_i}$ with $a_i, b_i \in \mathbb{Q}$; we have

  $$\lambda_1\lambda_3 = a_1a_3 + a_1b_3\sqrt{d_3} + a_3b_1\sqrt{d_1} + b_1b_3\sqrt{d_1d_3},$$

  and since $\lambda_1\lambda_3 = \lambda_2^2$ has degree at most 2 over $\mathbb{Q}$ there is a nontrivial element in $\mathrm{Gal}\,(F/\mathbb{Q})$ that fixes $\lambda_1\lambda_3$. Depending on this nontrivial element, we arrive at one of the following three possibilities: $a_1b_3 = a_3b_1 = 0$, $a_1b_3 = b_1b_3 = 0$, or $a_3b_1 = b_1b_3 = 0$. Since by assumption we have $2a_1 = \mathrm{tr}(\lambda_1) \neq 0$ and $2a_3 = \mathrm{tr}(\lambda_3) \neq 0$, these equations imply in all cases $b_1b_3 = 0$, but this contradicts the fact that $[\mathbb{Q}(\lambda_1) : \mathbb{Q}] = [\mathbb{Q}(\lambda_3) : \mathbb{Q}] = 2$.

$\square$

From now on we only consider primes $\ell \geq 5$. This ensures for example that the following definition is well posed ([BHRD13, Proposition 5.3.6 (ii)]):

Definition 13.3. We denote by $\mathrm{Sym}^4(\mathrm{SL}_2(\mathbb{F}_\ell))$ the image in $\Omega_5(\mathbb{F}_\ell)$ of the unique orthogonal representation of $\mathrm{SL}_2(\mathbb{F}_\ell)$ of dimension 5. The group $\mathrm{Sym}^4(\mathrm{SL}_2(\mathbb{F}_\ell))$ is well defined up to conjugation in $\Omega_5(\mathbb{F}_\ell)$.

Remark 13.4. We can give a concrete description of $\mathrm{Sym}^4(\mathrm{SL}_2(\mathbb{F}_\ell))$ as follows (cf. [BHRD13, Lemma 5.3.4]). Let $\varepsilon_0, \varepsilon_1$ be a basis of $\mathbb{F}_\ell^2$, and let $e_i = \varepsilon_0^{4-i}\varepsilon_1^i$ for $i = 0, \dots, 4$. Notice that $\mathrm{SL}_2(\mathbb{F}_\ell)$ is generated by

$$x(a) := \begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix}, \quad y(b) := \begin{pmatrix} b & 0 \\ 0 & b^{-1} \end{pmatrix}, \quad z := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},$$

and that these matrices together with

$$w(c) := \begin{pmatrix} c & 0 \\ 0 & 1 \end{pmatrix},\ c \in \mathbb{F}_\ell^\times$$

generate $\mathrm{GL}_2(\mathbb{F}_\ell)$. We let $\mathrm{GL}_2(\mathbb{F}_\ell)$ act (on the right) on $\mathbb{F}_\ell^5 \cong \bigoplus_{i=0}^4 \mathbb{F}_\ell \cdot e_i$ by the rule

$$e_i \cdot x(a) = \sum_{j=0}^{i} a^{i-j}\binom{i}{j} e_j, \quad e_i \cdot z = (-1)^i e_{4-i}, \quad e_i \cdot y(b) = b^{4-2i} e_i, \quad e_i \cdot w(c) = c^{4-i} e_i.$$

We denote the image of this representation by $\mathrm{Sym}^4(\mathrm{GL}_2(\mathbb{F}_\ell))$; the group $\mathrm{Sym}^4(\mathrm{SL}_2(\mathbb{F}_\ell))$ of the previous definition is the image of $\mathrm{SL}_2(\mathbb{F}_\ell)$ through this representation.

This explicit description shows that the action of a Borel subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$ on $\mathbb{F}_\ell^5$ fixes a 1-dimensional subspace: indeed up to conjugation we can assume that the Borel subgroup is generated by elements of the form $x(a), y(b), w(c)$, and it is clear from the explicit construction that this subgroup fixes the line spanned by e_0.

Lemma 13.5. *There is an effectively computable bound $\ell_2(A/K)$ with the following property: for every prime $\ell > \ell_2(A/K)$ the group G_ℓ contains $\mathrm{SL}_2(\mathbb{F}_\ell) \otimes \mathrm{Sym}^4(\mathrm{SL}_2(\mathbb{F}_\ell))$ (up to conjugacy).*

Proof. We proceed as in the proof of proposition 12.12. We can assume that (up to conjugacy) G_ℓ is contained in $\mathrm{GL}_2(\mathbb{F}_\ell)\otimes\mathrm{CGO}_5(\mathbb{F}_\ell)$, so we have well-defined projections π_2, π_5 to $\mathrm{PGL}_2(\mathbb{F}_\ell)$ and $\mathbb{P}\mathrm{CGO}_5(\mathbb{F}_\ell)$ respectively. We write $H_2 = \pi_2(G_\ell)$ and $H_5 = \pi_5(G_\ell)$.

It will be useful to take the following notation: when K' is a finite extension of K, we denote by $G_\ell^{(1)}$ the image of $\mathrm{Gal}\left(\overline{K'}/K'\right) \to \mathrm{Aut}\, A[\ell]$. It is a subgroup of G_ℓ, and therefore we can consider the restrictions of π_2, π_5 to $G_\ell^{(1)}$; we denote by $H_2^{(1)}$, resp. $H_5^{(1)}$, the image of the projection $\pi_2 : G_\ell^{(1)} \to \mathrm{PGL}_2(\mathbb{F}_\ell)$, resp. $\pi_5 : G_\ell^{(1)} \to \mathrm{PCGO}_5(\mathbb{F}_\ell)$. Notice now that, by the same argument as in the proof of proposition 12.12, for ℓ larger than $b_0(A/K)$ the groups H_2, H_5 do not stabilize linear subspaces; furthermore, for $\ell > b_0(A/K; 120)$ the image of H_2 cannot be contained in an exceptional subgroup of $\mathrm{PGL}_2(\mathbb{F}_\ell)$. It follows that (for these primes) H_2 contains either $\mathrm{PSL}_2(\mathbb{F}_\ell)$ or an abelian subgroup of index 2. On the other hand, table 8.22 of [BHRD13] reveals that all maximal subgroups of $\mathbb{P}\mathrm{CGO}_5(\mathbb{F}_\ell)$ not containing $\mathbb{P}\Omega_5(\mathbb{F}_\ell)$ – with the only exception of $\mathrm{Sym}^4(\mathrm{GL}_2(\mathbb{F}_\ell))$ – either stabilize some linear subspace or have order bounded by a constant K_5 independent of ℓ; the same arguments as in the proof of 12.12 show that H_5 cannot be contained in any such subgroup for $\ell > b_0(A/K; K_5)$. This leaves us with only two possibilities: either H_5 contains $\mathbb{P}\Omega_5(\mathbb{F}_\ell)$, or it is contained in the projective image of $\mathrm{Sym}^4(\mathrm{GL}_2(\mathbb{F}_\ell))$. We then have a total of four possibilities, according to the structure of H_2 and H_5. The case when H_5 contains $\mathbb{P}\Omega_5(\mathbb{F}_\ell)$ is easy to treat:

- if $H_2 \supseteq \mathrm{PSL}_2(\mathbb{F}_\ell)$, it is easy to see that G_ℓ contains $\mathrm{SL}_2(\mathbb{F}_\ell) \otimes \Omega_5(\mathbb{F}_\ell)$, which is even stronger than what we need.

- if H_2 has an abelian subgroup of index at most 2, then – as in the corresponding case in proposition 12.12 – we can replace K by a quadratic extension K' such that $H_2^{(1)}$ is abelian and $H_5^{(1)}$ contains $\mathrm{P}\Omega_5(\mathbb{F}_\ell)$. We then use Goursat's lemma to show that $G_\ell^{(1)}$ contains an element $\tilde{\alpha}$ such that $\pi_5(\tilde{\alpha}) = 1$ and $\pi_2(\tilde{\alpha})$ is nontrivial. Such an $\tilde{\alpha}$ is easily seen to be central in $G_\ell^{(1)}$, which in turn implies that the centralizer of $G_\ell^{(1)}$ in $\mathrm{End}\, A[\ell]$ is larger than $\mathbb{F}_\ell$: by proposition 4.1, this only happens for bounded values of ℓ.

We can then assume that H_5 is contained in the projective image of $\mathrm{Sym}^4(\mathrm{GL}_2(\mathbb{F}_\ell))$. Next notice that the maximal subgroups of $\mathbb{P}\,\mathrm{Sym}^4(\mathrm{GL}_2(\mathbb{F}_\ell)) \cong \mathrm{PGL}_2(\mathbb{F}_\ell)$ that do not contain $\mathrm{PSL}_2(\mathbb{F}_\ell)$ either stabilize a linear subspace (but this is impossible as long as $\ell > b_0(A/K)$), have order bounded by 120 (again, impossible for $\ell > b_0(A/K; 120)$), or have an abelian subgroup of index at most 2. Similar to what we know for H_2, it follows that H_5 contains either $\mathrm{Sym}^4(\mathrm{SL}_2(\mathbb{F}_\ell))$ or an abelian subgroup of index at most 2. We can now deal with the remaining cases.

- H_2 and H_5 both contain an abelian subgroup of index at most 2. Replacing K with an extension K' of degree at most 4, we can ensure that $G_\ell^{(1)}$ is abelian, which only happens for bounded values of ℓ (proposition 4.1).

- H_2 contains an abelian subgroup of index at most 2, H_5 contains $\mathbb{P}\operatorname{Sym}^4(\operatorname{SL}_2(\mathbb{F}_\ell))$. There is an extension K' of K, of degree at most 2, such that H_2' is abelian (and nontrivial) and H_5' contains $\mathbb{P}\operatorname{Sym}^4(\operatorname{SL}_2(\mathbb{F}_\ell))$: then Goursat's lemma shows that there is an element $\tilde{\alpha}$ of $G_\ell^{(1)}$ such that $\pi_5(\tilde{\alpha}) = \operatorname{Id}$ and $\pi_2(\tilde{\alpha})$ is nontrivial. But this implies that the centralizer of $G_\ell^{(1)}$ is larger than $\mathbb{F}_\ell$, which again only happens for bounded values of ℓ by proposition 4.1.

- H_2 contains $\operatorname{PSL}_2(\mathbb{F}_\ell)$, H_5 contains an abelian subgroup of index at most 2. We proceed as in the previous case, swapping the roles of H_5 and H_2.

- H_2 contains $\operatorname{PSL}_2(\mathbb{F}_\ell)$, H_5 contains $\mathbb{P}\operatorname{Sym}^4(\operatorname{SL}_2(\mathbb{F}_\ell))$. Since the groups $\mathbb{P}\operatorname{Sym}^4(\operatorname{SL}_2(\mathbb{F}_\ell))$ and $\operatorname{PSL}_2(\mathbb{F}_\ell)$ are both simple, an application of Goursat's lemma shows that only two subcases can arise: either $\mathbb{P}G_\ell$ contains all of $\operatorname{PSL}_2(\mathbb{F}_\ell) \otimes \mathbb{P}\operatorname{Sym}^4(\operatorname{SL}_2(\mathbb{F}_\ell))$, in which case we are done, or (up to replacing K with an extension K' of degree at most 4) $H_2^{(1)} \times H_5^{(1)}$ is the graph of an isomorphism $\operatorname{PSL}_2(\mathbb{F}_\ell) \to \mathbb{P}\operatorname{Sym}^4(\operatorname{SL}_2(\mathbb{F}_\ell))$. To complete the proof we have to show that this second case cannot arise for ℓ large enough, and once again we can use a method already employed in the proof of proposition 12.12. Namely, if $G_\ell^{(1)}$ is of this particular form, then the eigenvalues of any element of $G_\ell^{(1)}$ can be written as $\{\lambda_1, \lambda_2\} \otimes \{\lambda_1^4, \lambda_1^3\lambda_2, \lambda_1^2\lambda_2^2, \lambda_1\lambda_2^3, \lambda_2^4\}$ for some $\lambda_1, \lambda_2 \in \mathbb{F}_{\ell^2}$, but (for the same argument as in the proof of proposition 12.12) for ℓ large enough this is incompatible with the description of the action of the tame inertia I_w^t on $A[\ell]$ (where w is any place of K of characteristic ℓ). Notice that A has semistable reduction over K' at all places of characteristic different from 11: this follows from a theorem of Raynaud [GRR72, Proposition 4.7], because by assumption $A[11]$ is defined over K, and hence over K'.

□

Lemma 13.6. *There is an effectively computable bound $\ell_1(A/K)$ with the following property: there exists a prime $b(A/K) < \ell < \ell_1(A/K)$ such that G_ℓ contains $\operatorname{SL}_2(\mathbb{F}_\ell) \otimes \Omega_5(\mathbb{F}_\ell)$ (up to conjugacy).*

Proof. By the previous lemma, there is an effective bound $\ell_2(A/K)$ such that if $\ell > \ell_2(A/K)$ then G_ℓ contains $\operatorname{GL}_2(\mathbb{F}_\ell) \otimes \operatorname{Sym}^4(\operatorname{SL}_2(\mathbb{F}_\ell))$ (up to conjugacy). Let now ℓ_2 be the smallest prime larger than $\ell_2(A/K)$ (in particular, $\ell_2 \leq 2\ell_2(A/K)$) and let g_2 be an element of G_{ℓ_2} all of whose eigenvalues are distinct (it is easy to see that such an element exists). Let $v \in \Omega_K^A$ be such that Fr_v maps to g_2 in G_{ℓ_2}: thanks to the effective Chebotarev theorem, the residual characteristic of such a v can be bounded in terms of the discriminant of $K(A[\ell_2])$, which in turn can be bounded by an explicit function of Δ_K and $N_{K/\mathbb{Q}}\,\mathcal{N}^0_{A/K}$ (cf. the proof of theorem 12.17). We claim that one of the following holds (recall that $f_v(x)$ is the characteristic polynomial of Fr_v):

1. $f_v(x)$ does not factor (over $\mathbb{Q}$) as a product of polynomials of degree 2;

2. $f_v(x)$ does factor (over $\mathbb{Q}$) as a product of polynomials of degree 2, and the equation $\lambda_2^2 = \lambda_1\lambda_3$ has no solution $(\lambda_1, \lambda_2, \lambda_3)$ with $f_v(\lambda_i) = 0$ for $i = 1, 2, 3$ and $\lambda_1 \neq \lambda_2$ (that

is, this equation admits no nontrivial solutions if the unknowns are restricted to be eigenvalues of Fr_v).

Indeed, assume that (1) does not hold. Then $f_v(x)$ can be written as a product of quadratic factors, and all its roots $\mu_1, \ldots, \mu_{2g}$ are algebraic integers of degree 2 whose norm is $\sqrt{p_v}$. Now observe that every μ_j is congruent to 1 modulo 11 (since by assumption $A[11]$ is defined over K), so $\operatorname{tr} \mu_j \equiv 2 \pmod{11}$ is nonzero. Finally, lemma 12.1 implies that the subgroup of $\overline{\mathbb{Q}}^\times$ generated by the μ_j is torsion-free. Applying lemma 13.2 we see that if $\lambda_1, \lambda_2, \lambda_3$ are three roots of $f_v(x)$ that satisfy $\lambda_2^2 = \lambda_1\lambda_3$, then $\lambda_1 = \lambda_2 = \lambda_3$. But this is not possible: by construction, the eigenvalues of Fr_v are all distinct when regarded modulo ℓ_2, hence a fortiori they are all distinct in $\overline{\mathbb{Q}}$. The contradiction shows our claim. We now show that in both cases we can find a prime ℓ (explicitly bounded in terms of A and K) such that G_ℓ contains $\mathrm{SL}_2(\mathbb{F}_\ell) \otimes \Omega_5(\mathbb{F}_\ell)$.

1. Suppose first that (1) holds. Chebotarev's theorem yields the existence of a prime $\ell > \ell_2(A/K)$, smaller than some computable bound, such that the reduction of $f_v(x)$ in $\mathbb{F}_\ell[x]$ does not split completely over $\mathbb{F}_{\ell^2}$. Since $\ell > \ell_2(A/K)$, we know that G_ℓ either contains $\mathrm{SL}_2(\mathbb{F}_\ell) \otimes \Omega_5(\mathbb{F}_\ell)$ or is contained in $\mathrm{GL}_2(\mathbb{F}_\ell) \otimes \mathrm{Sym}^4(\mathrm{GL}_2(\mathbb{F}_\ell))$. In the second case, it is clear that the eigenvalues of any element of G_ℓ lie in $\mathbb{F}_{\ell^2}$, so the characteristic polynomial of any $h \in G_\ell$ splits completely over $\mathbb{F}_{\ell^2}$. However, for $h = \rho_\ell(\mathrm{Fr}_v)$ this is incompatible with our choice of ℓ, and the contradiction shows that G_ℓ contains $\mathrm{SL}_2(\mathbb{F}_\ell) \otimes \Omega_5(\mathbb{F}_\ell)$.

2. Suppose instead that (2) holds. For any triple μ_i, μ_j, μ_k of distinct eigenvalues of Fr_v, let $M(i,j,k) = |N_{F(v)/\mathbb{Q}}(\mu_j^2 - \mu_i\mu_k)|$, and let M be the least common multiple of all the $M(i,j,k)$. Since (2) holds, every $M(i,j,k)$ is a nonzero integer, and by the Weil conjectures each of them is bounded by a function of $q_v = p_v$; furthermore, M does not exceed $\prod_{i,j,k \text{ distinct}} M(i,j,k)$, so that ultimately M can be bounded by an effectively computable function of A/K. Now let ℓ be a prime larger than $\max\{M, \ell_2(A/K)\}$. As before, G_ℓ either contains $\mathrm{SL}_2(\mathbb{F}_\ell) \otimes \Omega_5(\mathbb{F}_\ell)$ or is contained in $\mathrm{GL}_2(\mathbb{F}_\ell) \otimes \mathrm{Sym}^4(\mathrm{GL}_2(\mathbb{F}_\ell))$. Observe however that in the second case the eigenvalues of any element $h \in G_\ell$ can be written as
$$\{\nu_1, \nu_2\} \otimes \{\xi_1^4,\ \xi_1^{4-1}\xi_2,\ \xi_1^2\xi_2^{4-2},\ \xi_1\xi_2^{4-1},\ \xi_2^4\}$$
for some $\nu_1, \nu_2, \xi_1, \xi_2 \in \mathbb{F}_{\ell^2}$, and in particular, we see that $h = \rho_\ell(\mathrm{Fr}_v)$ has three eigenvalues $\nu_1\xi_1^4, \nu_1\xi_1^{4-1}\xi_2$ and $\nu_1\xi_1^{4-2}\xi_2^2$ that satisfy $\left(\nu_1\xi_1^{4-1}\xi_2\right)^2 = \left(\nu_1\xi_1^4\right)\left(\nu_1\xi_1^{4-2}\xi_2^2\right)$. Now these three eigenvalues are the reduction in $\overline{\mathbb{F}_\ell}$ of three eigenvalues μ_j, μ_i, μ_k of Fr_v, which therefore satisfy $\overline{\mu_j}^2 = \overline{\mu_i}\,\overline{\mu_k} \in \overline{\mathbb{F}_\ell}$. However, by the same argument as in section 7, this implies that ℓ divides $|N_{F(v)/\mathbb{Q}}(\mu_j^2 - \mu_i\mu_k)| = M_{i,j,k}$, which in turn divides M by construction. This is a contradiction, and we thus see that in this case any prime larger than $\max\{M, \ell_2(A/K)\}$ satisfies the conclusion of the lemma. It is clear from our construction that such a prime can be bounded effectively in terms of A and K.

□

We are finally ready for the proof of proposition 13.1:

Proof. By the previous lemma, there is an effective bound $\ell_1(A/K)$ and a prime ℓ_1 with $b(A/K) < \ell_1 < \ell_1(A/K)$ such that G_{ℓ_1} contains $\mathrm{SL}_2(\mathbb{F}_\ell) \otimes \Omega_5(\mathbb{F}_\ell)$.

The inequality $\ell_1 > b(A/K)$ is easily seen to guarantee that $\mathrm{SL}_2(\mathbb{F}_\ell) \otimes \Omega_5(\mathbb{F}_\ell)$ contains an operator h_1 of tensor product type with weakly independent eigenvalues modulo ℓ_1, in the sense of definition 12.8. Let $v \in \Omega_K^A$ be a place of K such that Fr_v maps to h_1 in G_{ℓ_1}, and notice that the residual characteristic of v can be bounded effectively in terms of Δ_K and of $\mathcal{N}^0_{A/K}$. By an obvious variant of corollary 12.11, the Frobenius at v is not of tensor product type. We can then proceed as in the proof of theorem 1.6, thus obtaining an effective bound $\ell_0(A/K)$ as in the statement of the proposition. $\square$

14 A numerical example

In this short section we consider an explicit three-dimensional Jacobian and compute a bound on the largest prime for which G_ℓ can differ from $\mathrm{GSp}_6(\mathbb{F}_\ell)$. Zywina [Zyw15] has recently given an example of a three-dimensional Jacobian having maximal (adelic) Galois action, his approach consisting essentially in making effective a previous paper by Hall [Hal11] (see also the related work [ALS15]). Effective results based on Hall's techniques have also been obtained in [AAK$^+$14], where a sufficient condition is given that implies that the equality $G_\ell = \mathrm{GSp}_{2g}(\mathbb{F}_\ell)$ holds for a given abelian variety and a fixed prime ℓ. We recall that an abelian variety A/K satisfies Hall's condition if for some finite extension L of K and for some finite place v of L the fiber at v of the Néron model of $A/\mathcal{O}_L$ is semistable with toric-dimension equal to 1. Our example is fabricated precisely so as *not* to satisfy this condition, and is therefore – to the author's knowledge – the first abelian threefold not of Hall type for which the equality $G_\ell = \mathrm{GSp}_6(\mathbb{F}_\ell)$ is established for all primes larger than an explicit (albeit enormous) bound.

We now turn to the example itself. We consider the Jacobian A of a genus 3 hyperelliptic curve C over $\mathbb{Q}$, given in an affine patch by the equation $y^2 = g(x)$, where

$$g(x) = x^7 - x^6 - 5x^5 + 4x^4 + 5x^3 - x^2 - 5x + 3.$$

The polynomial $g(x)$ has been found by referring to [KM01]. We shall prove that A has potentially good reduction everywhere except at $q = 45427$, and that the reduction of $A/\mathbb{Q}$ at q is semistable of toric dimension 2. Let us start by remarking that the discriminant of $g(x)$ is q^2, so C is smooth (and A has good reduction) away from 2 and q. To study the exceptional places 2 and q we shall employ the *intersection graph* of a semistable model of C:

Definition 14.1. Let X be a semistable curve over an algebraically closed field K. The intersection graph $\Gamma(X)$ is the (multi)graph whose vertices are the irreducible components X_i of X and whose edges are the singular points of X/K: more precisely, a singular point $x \in X$ lying on X_i and X_j defines an edge between X_i and X_j (the case $i = j$ is allowed).

Theorem 14.2. *([BLR90, §9.2, Example 8]) Let X be a semistable curve over a field K. The semi-abelian variety $\mathrm{Pic}^0_{X/K}$ has toric dimension equal to $\operatorname{rank} H^1\left(\Gamma(X_{\overline{K}}), \mathbb{Z}\right)$.*

Notice now that we have $g(x) = (x+10504)^2(x+13963)^2\left(x^3 + 41919x^2 + 27613x + 35727\right)$ in $\mathbb{F}_q[x]$, so the reduction of C at q is semistable of toric dimension 2: indeed, our model has only ordinary double points as singularities, so the reduction is already semistable over $\mathbb{Q}_q$. Moreover, the curve is irreducible over $\overline{\mathbb{F}_q}$ and admits exactly two singular points, so the intersection graph is topologically the wedge of two copies of S^1, which shows that the toric dimension of the fiber at q is $\operatorname{rank} H^1\left(S^1 \vee S^1, \mathbb{Z}\right) = 2$. To study the reduction at 2 we shall need the following additional result:

Theorem 14.3. *([Mat03, Lemma 3.2.1] and [Ray90, Théorème 1']) Let K be a p-adic field with ring of integers R and denote v_p the corresponding p-adic valuation, extended to all of $\overline{K}$. Let X be the superelliptic curve given in the standard affine patch by the equation $y^p = \prod_{1\leq i\leq m}(x-x_i)$, where every x_i is in R and $(m,p)=1$. Suppose furthermore that $v_p(x_i) = v_p(x_i - x_j) = 0$ for every pair $i \neq j$. The intersection graph of the special fiber of the stable model $\mathcal{X}$ of X is a tree.*

Take K to be the field generated over $\mathbb{Q}_2$ by the roots x_i of $g(x)$: then C/K satisfies the hypotheses of theorem 14.3 for $p=2$, because $v_2\left(\prod x_i\right) = v_2(g(0)) = 0$ and

$$v_2\left(\prod_{i\neq j}(x_i - x_j)\right) = v_2(\operatorname{disc} g(x)) = 0.$$

Since trees have trivial H^1, applying theorem 14.2 we see that $\operatorname{Jac}(C/\mathbb{Q}_2)$ acquires good reduction over a finite extension of $\mathbb{Q}_2$: as claimed, A has potentially good reduction at 2. It follows in particular that A does not satisfy Hall's condition (over $\mathbb{Q}$, nor over any number field). Next we check that the Galois group of $g(x)$ is the full alternating group A_7, so by [Zar00, Theorem 2.1] we have $\operatorname{End}_{\overline{K}}(A) = \mathbb{Z}$. We then compute with Magma [BCP97] that the characteristic polynomial of the Frobenius at 3 is $f_3(x) = 27 + 9x^5 + 6x^2 + 2x^3 + 2x^4 + x^5 + x^6$, which has Galois group isomorphic to $(\mathbb{Z}/2\mathbb{Z})^3 \rtimes S_3$. It is interesting to observe that the characteristic polynomial of Fr_p has Galois group $(\mathbb{Z}/2\mathbb{Z})^3 \rtimes S_3$ at least for all odd primes up to 53 with the only exception of $p=17$: a random Frobenius usually has the largest possible Galois group, so that the corresponding place satisfies assumption (3) of theorem 1.2. Finally, we can use [Paz12, Théorème 2.4] to bound the Faltings height of A: the minimal discriminant of X does not exceed the discriminant of our model (namely $2^{12}q^2$, see [Paz12, Définition 8.1]), and (in the notation of [Paz12]) we can take $e_v = 0$ to get an upper bound on $h_F(A)$. Taking into account the normalization of the Faltings height used in [Paz12] we easily find that $h_F(A)$ does not exceed $-2.511...$ We now simply apply theorem 1.2 to $A/\mathbb{Q}$ and to the prime $v=3$ to deduce that $G_\ell = \operatorname{GSp}_6(\mathbb{F}_\ell)$ for all $\ell > \exp\left(3.8\cdot 10^8\right)$, this bound being much larger than the prime of bad reduction q.

Remark 14.4. The method of proof of proposition 7.5 produces a finite list of nonzero integers among whose prime divisors we can find all primes ℓ for which G_ℓ is of tensor product type. Carrying out these computations for Fr_3 rules out the possibility that G_ℓ is of tensor product type for any $\ell \geq 5$, and applying the same method to Fr_5 shows that G_3 is not of tensor product type either.

References

[AAK+14] S. Arias-de-Reyna, C. Armana, V. Karemaker, M. Rebolledo, L. Thomas, and N. Vila. Galois representations and Galois groups over $\mathbb{Q}$. *ArXiv e-prints*, July 2014.

[ALS15] S. Anni, P. Lemos, and S. Siksek. Residual Representations of Semistable Principally Polarized Abelian Varieties. *ArXiv e-prints*, August 2015.

[Asc84] M. Aschbacher. On the maximal subgroups of the finite classical groups. *Invent. Math.*, 76(3):469–514, 1984.

[BCP97] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[BHRD13] J. N. Bray, D. F. Holt, and C. M. Roney-Dougal. *The maximal subgroups of the low-dimensional finite classical groups*, volume 407 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 2013. With a foreword by Martin Liebeck.

[BLR90] S. Bosch, W. Lütkebohmert, and M. Raynaud. *Néron models*, volume 21 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]*. Springer-Verlag, Berlin, 1990.

[Bou02] N. Bourbaki. *Lie groups and Lie algebras. Chapters 4–6*. Elements of Mathematics (Berlin). Springer-Verlag, Berlin, 2002. Translated from the 1968 French original by Andrew Pressley.

[Bou08] N. Bourbaki. *Lie Groups and Lie Algebras: Chapters 7-9 (Elements of Mathematics)*. Springer Publishing Company, Incorporated, 2008.

[Car85] R. W. Carter. *Finite groups of Lie type*. Pure and Applied Mathematics (New York). John Wiley & Sons, Inc., New York, 1985. Conjugacy classes and complex characters, A Wiley-Interscience Publication.

[CCN$^+$85] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson. *Atlas of finite groups*. Oxford University Press, Eynsham, 1985. Maximal subgroups and ordinary characters for simple groups, With computational assistance from J. G. Thackray.

[Chi92] W. C. Chi. l-adic and λ-adic representations associated to abelian varieties defined over number fields. *Amer. J. Math.*, 114(2):315–353, 1992.

[Col08] M. J. Collins. Modular analogues of Jordan's theorem for finite linear groups. *J. Reine Angew. Math.*, 624:143–171, 2008.

[Die02] L. V. Dieulefait. Explicit determination of the images of the Galois representations attached to abelian surfaces with $\mathrm{End}(A) = \mathbb{Z}$. *Experiment. Math.*, 11(4):503–512 (2003), 2002.

[GLT12] R. Guralnick, M. Larsen, and P. H. Tiep. Representation growth in positive characteristic and conjugacy classes of maximal subgroups. *Duke Math. J.*, 161(1):107–137, 2012.

[GR14] É. Gaudron and G. Rémond. Polarisations et isogénies. *Duke Math. J.*, 163(11):2057–2108, 2014.

[Gri73] R. Griess. Schur multipliers of finite simple groups of Lie type. *Trans. Amer. Math. Soc.*, 183:355–421, 1973.

[Gro] A. Grothendieck. Modèles de Néron et monodromie. In *Séminaire de Géométrie Algébrique, Volume 7, Esposé 9.*

[GRR72] A. Grothendieck, M. Raynaud, and D. S. Rim. *Groupes de monodromie en géométrie algébrique. I.* Lecture Notes in Mathematics, Vol. 288. Springer-Verlag, 1972. Séminaire de Géométrie Algébrique du Bois-Marie 1967–1969 (SGA 7 I).

[Hal11] C. Hall. An open-image theorem for a general class of abelian varieties. *Bull. Lond. Math. Soc.*, 43(4):703–711, 2011. With an appendix by Emmanuel Kowalski.

[HP15] M. Hindry and A. Pacheco. An analogue of the Brauer-Siegel theorem for abelian varieties in positive characteristic. *Moscow Math. J.*, 2015. To appear. Available at `https://sites.google.com/site/amilcarpachecoresearch/publications`.

[Hum78] J. E. Humphreys. *Introduction to Lie algebras and representation theory*, volume 9 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Berlin, 1978. Second printing, revised.

[Hum06] J. E. Humphreys. *Modular representations of finite groups of Lie type*, volume 326 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 2006.

[Jan97] J. C. Jantzen. Low-dimensional representations of reductive groups are semisimple. In *Algebraic groups and Lie groups*, volume 9 of *Austral. Math. Soc. Lect. Ser.*, pages 255–266. Cambridge Univ. Press, Cambridge, 1997.

[KL90] P. Kleidman and M. Liebeck. *The subgroup structure of the finite classical groups*, volume 129 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 1990.

[KM01] J. Klüners and G. Malle. A database for field extensions of the rationals. *LMS J. Comput. Math.*, 4:182–196 (electronic), 2001.

[Lie85] M. Liebeck. On the orders of maximal subgroups of the finite classical groups. *Proc. London Math. Soc. (3)*, 50(3):426–446, 1985.

[LO77] J. C. Lagarias and A. M. Odlyzko. Effective versions of the Chebotarev density theorem. In *Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975)*, pages 409–464. Academic Press, London, 1977.

[Lom14] D. Lombardo. Explicit surjectivity for Galois representations attached to abelian surfaces. *ArXiv e-prints*, November 2014.

[Lom15] D. Lombardo. Bounds for Serre's open image theorem for elliptic curves over number fields. *Algebra and Number Theory*, 2015. To appear.

[LP11] M. J. Larsen and R. Pink. Finite subgroups of algebraic groups. *J. Amer. Math. Soc.*, 24(4):1105–1158, 2011.

[Lüb01] F. Lübeck. Small degree representations of finite Chevalley groups in defining characteristic. *LMS J. Comput. Math.*, 4:135–169 (electronic), 2001.

[LV14] E. Larson and D. Vaintrob. Determinants of subquotients of Galois representations associated with abelian varieties. *J. Inst. Math. Jussieu*, 13(3):517–559, 2014. With an appendix by B. Conrad.

[Mat03] M. Matignon. Vers un algorithme pour la réduction stable des revêtements p-cycliques de la droite projective sur un corps p-adique. *Math. Ann.*, 325(2):323–354, 2003.

[McN98] G. J. McNinch. Dimensional criteria for semisimplicity of representations. *Proc. London Math. Soc. (3)*, 76(1):95–149, 1998.

[MNR89] J.-P. Massias, J.-L. Nicolas, and G. Robin. Effective bounds for the maximal order of an element in the symmetric group. *Math. Comp.*, 53(188):665–678, 1989.

[Mum69] D. Mumford. A note of Shimura's paper "Discontinuous groups and abelian varieties". *Math. Ann.*, 181:345–351, 1969.

[MW93a] D. Masser and G. Wüstholz. Isogeny estimates for abelian varieties, and finiteness theorems. *Ann. of Math. (2)*, 137(3):459–472, 1993.

[MW93b] D. W. Masser and G. Wüstholz. Galois properties of division fields of elliptic curves. *Bull. London Math. Soc.*, 25(3):247–254, 1993.

[MW93c] D. W. Masser and G. Wüstholz. Periods and minimal abelian subvarieties. *Ann. of Math. (2)*, 137(2):407–458, 1993.

[Œ79] J. Œsterlé. Versions effectives du théorème de Chebotarev sous l'hypothèse de Riemann généralisée. In *Journées Arithmétiques de Luminy (Colloq. Internat. CNRS, Centre Univ. Luminy, Luminy, 1978)*, volume 61 of *Astérisque*, pages 165–167. Soc. Math. France, Paris, 1979.

[Paz12] F. Pazuki. Décompositions en hauteurs locales. *ArXiv e-prints*, May 2012.

[Paz15] F. Pazuki. Heights, ranks and regulators of abelian varieties. *ArXiv e-prints*, June 2015.

[Pin98] R Pink. ℓ-adic algebraic monodromy groups, cocharacters, and the Mumford-Tate conjecture. *J. reine angew. Math*, (495), 1998.

[Pre87] A. A. Premet. Weights of infinitesimally irreducible representations of Chevalley groups over a field of prime characteristic. *Mat. Sb. (N.S.)*, 133(175)(2):167–183, 271, 1987.

[Ray74] M. Raynaud. Schémas en groupes de type $(p, \ldots, p)$. *Bull. Soc. Math. France*, 102:241–280, 1974.

[Ray90] M. Raynaud. p-groupes et réduction semi-stable des courbes. In *The Grothendieck Festschrift, Vol. III*, volume 88 of *Progr. Math.*, pages 179–197. Birkhäuser Boston, Boston, MA, 1990.

[Sen73] S. Sen. Lie algebras of Galois groups arising from Hodge-Tate modules. *Ann. of Math. (2)*, 97:160–170, 1973.

[Ser81] J.-P. Serre. Quelques applications du théorème de densité de Chebotarev. *Inst. Hautes Études Sci. Publ. Math.*, (54):323–401, 1981.

[Ser86] J.-P. Serre. Résumé des cours de 1985-1986, Annuaire du Collège de France, 1986.

[Ser00a] J.-P. Serre. Letter to M-F. Vigneras, January 1^{st}, 1983. In *Œuvres. Collected papers. IV*. Springer-Verlag, Berlin, 2000.

[Ser00b] J.-P. Serre. Résumé des cours au Collège de France, 1984-1985. In *Œuvres. Collected papers. IV*, pages viii+657. Springer-Verlag, Berlin, 2000. 1985–1998.

[Ste63] R. Steinberg. Representations of algebraic groups. *Nagoya Math. J.*, 22:33–56, 1963.

[Ste68] R. Steinberg. *Lectures on Chevalley groups*. Yale University, New Haven, Conn., 1968. Notes prepared by John Faulkner and Robert Wilson.

[TZ14] D. Testerman and A. Zalesski. Subgroups of simple algebraic groups containing regular tori, and irreducible representations with multiplicity 1 non-zero weights. *ArXiv e-prints*, March 2014.

[Vas03] A. Vasiu. Surjectivity criteria for p-adic representations. I. *Manuscripta Math.*, 112(3):325–355, 2003.

[Win] B. Winckler. Letter to the author.

[Won72] W. J. Wong. Irreducible modular representations of finite Chevalley groups. *J. Algebra*, 20:355–367, 1972.

[Zam15] A. Zaman. Bounding the least prime ideal in the Chebotarev Density Theorem. *ArXiv e-prints*, August 2015.

[Zar00] Yu. G. Zarhin. Hyperelliptic Jacobians without complex multiplication. *Math. Res. Lett.*, 7(1):123–132, 2000.

[Zyw15] D. Zywina. An explicit Jacobian of dimension 3 with maximal Galois action. 2015. Available from `http://www.math.cornell.edu/~zywina/`.